

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual;)
)
COALITION FOR GOOD)
GOVERNANCE, a non-profit corporation)
organized and existing under Colorado)
Law;)
)
DONNA PRICE, an individual;)
)
JEFFREY SCHOENBERG, an individual;)
)
LAURA DIGGES, an individual;)
)
WILLIAM DIGGES III, an individual;)
)
RICARDO DAVIS, an individual;)
)
Plaintiffs,)
)
v.)
)
BRIAN P. KEMP, in his individual)
capacity and his official capacity as)
Secretary of State of Georgia and)
Chair of the STATE ELECTION BOARD;)
)
DAVID J. WORLEY, REBECCA N.)
SULLIVAN, RALPH F. “RUSTY”)
SIMPSON, and SETH HARP, in their)
individual capacities and their official)
capacities as members of the STATE)
ELECTION BOARD;)

CIVIL ACTION 2017CV292233
FILE NO.:

**DEMAND FOR
JURY TRIAL**

)
THE STATE ELECTION BOARD;)
)
RICHARD BARRON, in his individual)
capacity and his official capacity as)
Director of the FULTON COUNTY)
BOARD OF REGISTRATION AND)
ELECTIONS;)
)
MARY CAROLE COONEY, VERNETTA)
NURIDDIN, DAVID J. BURGE, STAN)
MATARAZZO and AARON JOHNSON)
in their individual capacities and official)
capacities as members of the FULTON)
COUNTY BOARD OF REGISTRATION)
AND ELECTIONS;)
)
THE FULTON COUNTY BOARD OF)
REGISTRATION AND ELECTIONS;)
)
MAXINE DANIELS, in her individual)
capacity and her official capacity as)
Director of VOTER REGISTRATIONS)
AND ELECTIONS FOR DEKALB)
COUNTY;)
)
MICHAEL P. COVENY, ANTHONY)
LEWIS, LEONA PERRY, SAMUEL)
E. TILLMAN, and BAOKY N. VU)
in their individual capacities and official)
capacities as members of the DEKALB)
COUNTY BOARD OF REGISTRATIONS)
AND ELECTIONS;)
)
THE DEKALB COUNTY BOARD OF)

REGISTRATIONS AND ELECTIONS;)
)
JANINE EVELER, in her individual)
capacity and her official capacity as)
Director of the COBB COUNTY)
BOARD OF ELECTIONS AND)
REGISTRATION;)
)
PHIL DANIELL, FRED AIKEN, JOE)
PETTIT, JESSICA BROOKS, and)
DARRYL O. WILSON in their individual)
capacities and official capacities as)
members of the COBB COUNTY)
BOARD OF ELECTIONS AND)
REGISTRATION;)
)
THE COBB COUNTY BOARD OF)
ELECTIONS AND REGISTRATION;)
)
MERLE KING, in his individual capacity)
and his official capacity as Executive)
Director of the CENTER FOR ELECTION)
SYSTEMS AT KENNESAW STATE)
UNIVERSITY; and)
)
THE CENTER FOR ELECTION)
SYSTEMS AT KENNESAW STATE)
UNIVERSITY)
)
Defendants.)

**VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE
RELIEF, AND WRIT OF MANDAMUS**

COMES NOW, Plaintiffs, named above, to show this Honorable Court the following for their Complaint against the above-named Defendants:

I. INTRODUCTION

This is a case about the insecurity of Georgia's voting system, and those who are responsible for ensuring its security. Because of the insecurity of Georgia's voting system and the lack of voter-verifiable paper ballots, the precise outcome of the June 20, 2017 Runoff Election between Karen Handel and Jon Ossoff for Georgia's 6th Congressional District ("Runoff") cannot be known. This uncertainty, which violates the rights of those who cast their ballots, was caused by the Defendants' misconduct, negligence, abuse of discretion, and noncompliance with the federal Constitution, federal law, the Georgia Constitution and Georgia law.

1.

In August of 2016 Logan Lamb ("Lamb"), a professional cybersecurity researcher curious about the Center for Election Systems at Kennesaw State University ("CES"), which is responsible for overseeing, maintaining, and securing the electronic election infrastructure for the state of Georgia, discovered that he was able to access key parts of Georgia's electronic election infrastructure through

CES's public website on the internet. Affidavit of Logan Lamb, June 30, 2017, attached as "Exhibit A."

2.

Lamb immediately alerted CES to the serious security vulnerabilities that he had discovered, advising CES that they should "Assume any document that requires authorization has already been downloaded without authorization." Exhibit A at ¶5.

3.

CES did not secure the vulnerabilities. Exhibit A at ¶7.

4.

Lamb had discovered that CES had improperly configured its server and had failed to patch a security flaw that had been known since 2014. These mistakes allowed anyone to access the internal information stored on CES's servers. Those documents included "a database containing registration records for the state's 6.7 million voters; multiple PDFs with instructions and passwords for election workers to sign in to a central server on Election Day; and software files for the state's ExpressPoll pollbooks — electronic devices used by pollworkers [sic.] to verify that a voter is registered before allowing them to cast a ballot. There also appeared to be databases for the so-called GEMS servers. These Global Election

Management Systems are used to prepare paper and electronic ballots, tabulate votes and produce summaries of vote totals.”¹ Exhibit A at ¶4.

5.

Lamb discovered that he could access via the internet all of Georgia’s voter registration records, including personally identifiable information, documents with election day passwords to access the central server for the election, and the code that was to be used to run the election. This information was everything a bad actor (such as a hacker) would need in order to interfere with the election.

6.

It is unknown how long CES had left this data exposed before Lamb discovered it.

7.

In addition, the documents Lamb discovered included training videos, at least one of which “instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.” Exhibit A at ¶11. Such a procedure would result in election workers ensuring that whatever code existed on CES’s website ended up on voting machines. This would be a serious security concern,

¹ Kim Zettler, Will the Georgia Special Election Get Hacked, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>, (last visited June 30, 2017)

creating the possibility of malicious software being uploaded to voting machines in Georgia, if CES's servers were compromised, as in fact they were.

8.

Georgia law explicitly allows the Secretary of State to, "at any time, in his or her discretion," reexamine the voting machines used in Georgia, and to prevent their use if they "can no longer be safely and accurately used." O.C.G.A § 21-2-379.2. Despite this, CES and the Secretary of State allowed elections in 2016 and 2017 to be run on this compromised system with the knowledge that they could not be presumed to be able to be "safely or accurately used by electors." Id.

9.

It is presently unknown if any party interfered with Georgia's elections in 2016 or 2017. But according to then-Director of the Federal Bureau of Investigation ("FBI"), James Comey, hackers were "scanning" election systems in the lead up to the election in the fall of 2016.² Subsequent reporting has suggested that as many as 39 states were targeted.³ Secretary of State Brian Kemp ("Kemp"), through his spokesman, denied that Georgia was one of the states so targeted.⁴

² Kristina Torres, Georgia Not One of 20 States Targeted by Hackers Over Election Systems, Atlanta Journal Constitution, September 30, 2016, (<http://www.ajc.com/news/state--regional-govt--politics/georgia-not-one-states-targeted-hackers-over-election-systems/FvCGGjulVUm7VNMP8a9vuO/>) (last visited June 30, 2017)

³ Michael Riley and Jordan Robertson, Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known, BloombergPolitics, June 13, 2017,

10.

What is known is that the United States Department of Homeland Security (“DHS”) held a call with election officials to discuss cybersecurity concerning the election in August 2016. At this time, DHS offered assistance to any state that wanted help securing its electronic election infrastructure.⁵ Kemp, on behalf of Georgia, refused that offer of assistance to secure Georgia’s voting systems.⁶ Kemp said the offer amounted to an attempt to “subvert the Constitution to achieve the goal of federalizing elections under the guise of security.”⁷

11.

Despite the warning from DHS, upon information and belief, no responsible official or entity, including Kemp, CES, or any election official, took action to ensure the security of Georgia’s election infrastructure.

<https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections> (Last visited June 30, 2017)

⁴ Kristina Torres, State Considers Dropping Election Data Center, Atlanta Journal Constitution, June 14, 2017, <http://www.myajc.com/news/state--regional-govt--politics/state-considers-dropping-election-data-center/YLERatmHYmLEqnOjUng2GL/> (last visited June 30, 2017)

⁵ DHS Press Office, Readout of Secretary Johnson’s Call With State Election Officials on Cybersecurity, Department of Homeland Security, August 15, 2016, <https://www.dhs.gov/news/2016/08/15/readout-secretary-johnsons-call-state-election-officials-cybersecurity> (last visited June 30, 2017)

⁶ Marshall Cohen and Tom LoBianco, Hacking the Election? Feds Step in as States Fret Cyber Threats, CNN, September 23, 2016, <http://www.cnn.com/2016/09/23/politics/ohio-pennsylvania-election-2016-hack/index.html>, (last visited June 30, 2017)

⁷ *Id.*

12.

Seven months after Lamb was able to access critical information concerning Georgia's voting systems via CES's publicly available website on the internet, another researcher was able to do the same. On or about March 1, 2017, Chris Grayson ("Grayson"), a colleague of Lamb's, discovered that CES had not fixed all of the security issues identified by Lamb in August 2016. That is, from at least August of 2016 to March of 2017 – a time period that overlapped with known attempts by Russia to hack elections in the United States – CES left exposed for anyone on the internet to see and potentially manipulate: voter registration records, passwords for the central server, and election related applications.⁸

13.

Lamb confirmed Grayson's findings and determined that he was able to download information he had accessed in August 2016, as well as new information which had since been uploaded. Exhibit A at ¶8.

14.

The newly discovered information included more recent files related to software, information related to the 2016 Presidential election, and files dated 2017. Exhibit A at ¶8.

⁸ Kim Zetter, Will the Georgia Special Election Get Hacked, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255> (last visited June 30, 2017).

15.

When Lamb notified CES directly of the issue in August 2016, Merle King, the Executive Director of CES, allegedly told him, “It would be best if you were to drop this now,” and warned that if Lamb did talk “the people downtown, the politicians … would crush [him].”⁹

16.

This time in March 2017, rather than notifying CES directly, Grayson notified Andrew Green, a colleague and a faculty member at Kennesaw State University (“KSU”). Email Chris Grayson to Andrew Green, March 2, 2017, attached as “Exhibit B.” On information and belief, Mr. Green notified KSU’s University Information Technology Services (“UITS”) Information Security Office, which in turn appears to have notified CES. KSU’s UITS Information Security Office is not directly affiliated with CES. KSU UITS Information Security Office, “Incident Report,” April 18, 2017, attached as “Exhibit C.”

17.

Within an hour of Grayson’s notification, the KSU UITS Information Security Office established a firewall to isolate CES’s server. Exhibit C, pages 1-2. It is not known why such action was not taken by CES after Lamb’s notification in August 2016.

⁹ Id.

18.

The day after Grayson's notification, the KSU UITS Information Security Office seized CES's server to preserve evidence "for later analysis and handoff to federal authorities." Exhibit C, page 2. It is not known why such action was not taken by CES after Lamb's notification in August 2016.

19.

Two days after Grayson's notification, the FBI was alerted and took possession of the server. Exhibit C, page 1. It is not known why such action was not taken by CES after Lamb's notification in August 2016.

20.

CES's information technology staff, which had previously been outside of KSU's Information Security Office, were then "realigned" to be a part of KSU's information security structure. Exhibit C, page 1. It is not known why such action was not taken after Lamb's notification in August 2016.

21.

Following the realignment, CES's information technology staff conducted a walkthrough, a cursory examination of the physical IT structure, with the KSU UITS Information Security Office. Exhibit C, page 1. This review led to the elections backup server also being physically removed. Id. It is not known why such action was not taken after Lamb's notification in August 2016.

22.

The walkthrough revealed numerous other security failures at CES. Exhibit C, pages 3-4. These failures included the absence of a working lock on the door to the private elections server closet, the presence of a wireless access point in the CES facility, and live access to an external network in the private network closet.

Id.

23.

The “Incident Report” also found that no security assessment had been done on the supposedly isolated CES network. Exhibit C, page 4.

24.

CES was first alerted to Grayson’s access to their systems on March 1, 2017. The “Incident Report” on this matter was completed on April 18, 2017 – which happened to be the date of the Special Election for Georgia’s 6th Congressional District (“Special Election”).

25.

Georgia law explicitly allows the Secretary of State to, “at any time, in his or her discretion,” reexamine the voting machines used in Georgia, and to prevent their use if they “can no longer be safely and accurately used.” O.C.G.A § 21-2-379.2. Despite this, CES, the Secretary of State, and other Defendants allowed the April 18, 2016 Special Election to be run on this compromised system with the

knowledge that they could not be presumed to be able to be “safely or accurately used by electors”. Id. Furthermore, the Various County Board of Elections and Registration Defendants had the authority to use paper ballots when a voting system is impracticable to use. O.C.G.A. §21-2-218.

26.

Despite this authority, duty, and ability to avoid unsafe systems, the Defendants allowed the Special Election to be run on a compromised system. Despite the knowledge of this compromised system, the Defendants refused to use the only safe method for conducting the election—paper ballots. This is especially important because Georgia uses a Direct Electronic Recording (“DRE”) voting machine, along with various voting, and tabulation programs that, when working properly, directly record an elector’s vote on an electronic medium but do not produce a paper record that is verifiable by the voter (“Georgia’s DRE-Based Voting System”).

27.

While Lamb and Grayson’s access to CES’s supposedly secure systems was being investigated, others were sounding the alarm about the security of Georgia’s elections infrastructure with the nationally watched Special Election

and the June 20, 2017 Runoff Election for Georgia's 6th Congressional District ("Runoff") pending.

28.

For example, on March 15, 2017, a group over 20 experts in the field of computer security and voting systems sent a letter to Kemp expressing their concerns with the security of Georgia's election systems in light of the reported breach at CES.¹⁰ And on March 16, 2017, the Democratic Party of Georgia, also responding to those reports, wrote Kennesaw State University, and copied Kemp, expressing concerns over the security of the election.¹¹

29.

None of these warnings appear to have resulted in any remedial action on the part of any of the Defendants.

30.

On April 15, 2017, an additional known security breach occurred when electronic poll books, containing a voter registration database and software to program voter access cards, were stolen from an election worker's truck where he

¹⁰ Verified Voting Blog: Technology Experts' Letter to Georgia Secretary of State Brian Kemp, VerifiedVoting, March 14, 2017, <https://www.verifiedvoting.org/verified-voting-letter-to-georgia-secretary-of-state-brian-kemp/> (last visited June 30, 2017)

¹¹ Letter from Chairman DuBose Porter, Democratic Party of Georgia to President Samuel S. Olens, Kennesaw State University, March 16, 2017, <http://www.georgiademocrat.org/wp-content/uploads/2017/03/KSU-Letter-of-Request-031617.pdf> (last visited June 30, 2017)

had left them unattended while grocery shopping.¹² The Chairman of the Cobb County GOP was quoted as saying that, “The theft could just be a random thing, but the timing makes it much more worrisome, [...] I think there is cause to be concerned about the integrity of the elections.”¹³ Poll books are used to confirm the voter’s name and address and to create a voter access card that has key information on it, information used to indicate the ballot style to which that voter is entitled to vote.

31.

This theft of electronic poll books did not cause Kemp to take any action such as decertifying the DRE-Based Voting System or calling for the use of paper ballots, nor did it cause any of the other Defendants to fulfill their duty to employ a safe and legal system of voting on paper ballots.

32.

The Special Election experienced technical problems, including voters being sent from one precinct to another and then back to their original precincts due to glitches in the electronic poll book software.¹⁴ Another error caused by the

¹² Christopher Wallace, New details emerge in theft of Ga. Voting machines, Fox News April 18, 2017, <http://www.foxnews.com/politics/2017/04/18/new-details-emerge-in-theft-ga-voting-machines.html>, (last visited June 30, 2017.)

¹³ Id.

¹⁴ Kim Zetter, Will the Georgia Special Election Get Hacked, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>, (last visited June 30, 2017)

uploading of improper and unauthorized memory cards—something the system is not supposed to allow—resulted in errors and delays in uploading election results.¹⁵ These errors were sufficiently severe that Kemp called for an investigation into them.¹⁶ No results from this investigation have been announced, nor has the public been told that it has been completed. Yet with that pending investigation ongoing, the Defendants instructed that the Runoff be conducted on the same voting system.

33.

On May 10, 2017, based on the publicly available information, and fearing that the Runoff could be compromised, a group of Georgia electors utilized their rights under O.C.G.A §21-2-379.2¹⁷ and requested that Georgia’s DRE-Based Voting System be reexamined. On May 15, 2017, a second letter was sent explaining the irreversible security issues in the system and a request that the voting system be reexamined. Two additional letters followed, on May 19 and June 2, requesting a timely response. No answer was received until after the electors

¹⁵ Arielle Kass, ‘Rare Error’ Delays Fulton County Vote Counts in 6th District Race, Atlanta Journal Constitution, April 19, 2017, <http://www.ajc.com/news/local-govt--politics/rare-error-delays-fulton-county-vote-counts-6th-district-race/dleYXJvjL1R9gSsw1swwAJ/> (last visited June 30, 2017)

¹⁶ Aaron Diamant and Berndt Petersen, State Opens Investigation into Issues With 6th District Race, WSBTV, May 26, 2017, <http://www.wsbtv.com/news/local-atlanta/state-opens-investigation-into-issues-with-6th-district-race/514213222> (last accessed June 30, 2017)

¹⁷ “Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any such system previously examined and approved by him or her.”

filed suit on May 25 against Kemp over his lack of response. See Curling v. Kemp, Case No. 2017CV290630.

34.

The Secretary of State's Office did not respond to the elector's requests until June 5, 2017. It indicated that it would complete the reexamination in approximately six months, putting the completion date after the date of elections that will be held in November. Letter from C. Ryan Germany to various electors, June 5, 2017, attached as "Exhibit D."

35.

Pending the reexamination, and despite the fact that Georgia law allows for voting to be done by paper ballot if the electronic system is unusable, the Secretary of State declined to use his authority under O.C.G.A §21-2-379.2 to prevent the use of voting machines for the Runoff. Exhibit D. The County Defendants likewise declined to use their authority under O.C.G.A. § 21-2-334 or § 21-2-28 to issue paper ballots for the Runoff.

36.

Notwithstanding the known problems – known incidents of unauthorized access into Georgia's election system, the known lax security, concerns about potentially undetected breaches, the stolen electronic poll books, other security failures, glitches in the Special Election pollbook operations, known errors in the

April 18 tabulation process, and the pending request for reexamination – the Defendants all allowed the Runoff to be conducted using Georgia’s DRE-Based Voting System, rather than by paper ballot.

37.

All of this took place against the backdrop of Georgia’s election systems being particularly vulnerable as has been documented for 15 years by voting system experts and computer scientists.

38.

The State of Georgia uses a Direct-Recording Electronic (“DRE”)-based voting system to conduct its elections. DRE machines, when working properly, directly record a voter’s ballot choices to an electronic storage medium for tabulation. DRE voting machines, unlike other voting methods, do not allow voters to verify that their votes have been correctly recorded and do not create auditable paper records of how votes were cast. Affidavit of Edward W. Felten, ¶¶5-6, attached as “Exhibit E.” This absence of a paper trail is the reason “computer scientists and cybersecurity experts typically recommend against the use of DREs.” Id. at ¶7.

39.

Security researchers have repeatedly demonstrated that the hardware and software of these types of machines is vulnerable to hacking. Exhibit E. For example, in 2006, security researchers from Princeton, including Edward W. Felten, were able to hack an AccuVote TS, the primary machine in use in Georgia, in under four minutes using just \$12 worth of tools.¹⁸ This hack allowed them to infect a single AccuVote TS machine in a way that would spread to the total election results when the device's memory card was used to tabulate the results.¹⁹ They were able to prove that these machines could be physically hacked in a matter of minutes, that malicious software could be installed, and that malicious software could then spread.²⁰ See Exhibit E. Since these machines do not provide a voter-verified paper ballot, there is no independent method to confirm that votes were counted, and counted as cast.

40.

Because of security concerns, several states have decertified these voting machines and/or the software running on them. For example, in 2006 Maryland's

¹⁸ Daniel Turner, How to Hack an Election in One Minute, MIT Technology Review, September 18, 2016, <https://www.technologyreview.com/s/406525/how-to-hack-an-election-in-one-minute/> (last visited June 30, 2016).

¹⁹ Id.

²⁰ Id.

House of Delegates voted unanimously to stop using these machines²¹ and in 2009 the Secretary of State for the State of California decertified the code running on them, GEMS 1.18.19.²² The version of GEMS that California decertified was only three minor revisions earlier than the version of GEMS now being used in Georgia, GEMS 1.18.22.G!.

41.

The security problems are exacerbated by the age of Georgia's voting machines, which are more than a decade old and run on antiquated software. Electronic voting devices over ten years old are generally understood to have surpassed their expected life span, after which core components begin to break or malfunction.²³ Worse, as the Brennan Center for Justice notes, older machines have more security vulnerabilities than newer devices and so are more susceptible to hacking and outside interference. Further, they tend to run outdated software on

²¹ Common Sense in Maryland, New York Times, March 23, 2006, <http://www.nytimes.com/2006/03/23/opinion/common-sense-in-maryland.html?mcubz=1> (last visited June 30, 2017)

²² Withdrawal of Approval of Premier Election Solutions, Inc./Diebold Election Systems, Inc., GEMS 1.18.19, Office of the Secretary of State of the State of California, March 30, 2009, <http://votingsystems.cdn.sos.ca.gov/vendors/premier/premier-11819-withdrawal-approval033009.pdf> (last visited June 30, 2017)

²³ Kristina Torres, An Election Primer on Georgia's Voting System and Ballot Security, Atlanta Journal Constitution, September 9, 2016, <http://www.myajc.com/news/state--regional-govt--politics/election-primer-georgia-voting-system-and-ballot-security/yedbpzowTMxdeBOwjHlkZP> (last visited June 30, 2017)

outdated and no longer manufactured hardware leading to additional difficulties and security issues.²⁴

42.

These problems are exacerbated by the fact that Georgia uses just one kind of machine, running one set of software for its elections, programmed by and downloaded from one central location—CES. Exhibit E at ¶26. This makes Georgia far easier to target than states that use multiple systems distributed and managed at a county level across the state, as only one vulnerability needs to be exploited. The public knows that the system was vulnerable because two researchers accessed it from the internet. In Georgia, a bad actor could manipulate the state’s electoral process by targeting and infiltrating CES.

43.

The fact that the electronic infrastructure is centralized at a single location, CES, provides an additional point of vulnerability. Since CES exposed passwords to the server, exposed code, left key rooms unlocked, and permitted unauthorized internet access, a malicious hacker could tamper with the election tabulation programming and results. See Exhibit A and Exhibit C. In other states, a single

²⁴https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf pages 12-17).

point of failure would not render the entire state's election suspect as most use decentralized--and properly certified and operated--systems.

44.

The DRE-Based Voting System used by Georgia creates no paper trail by which the accuracy of the vote can be verified. See Exhibit E. There is no physical record to ensure that votes are counted, and counted as cast.

45.

As Dr. Felten notes, "Because of the vulnerability of the DRE voting machines to software manipulation, and because of the intelligence reports about highly skilled cyber-attackers having attempted to affect elections in the United States, [stringent] precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism." Exhibit E at ¶ 29.

46.

Georgia began using a DRE-based system to conduct its elections in 2002. The devices used were certified for use by the then Secretary of State, Cathy Cox. Certification of Election Systems for use in Georgia, attached as "Exhibit F." Secretary of State Cox again certified these systems in 2003, 2004, 2005, and

2006. Id. Her successor, Karen Handel, certified the system that was used in 2007. Id. An examination of the certifications on file suggests that this is the last time a Georgia Secretary of State certified the voting system in use—albeit without explicitly opining on the safety and accuracy of the voting system of the State of Georgia, as is further required by §21-2-379.2 (a).

47.

Kemp has not once--in the past seven years of his two terms in office as Secretary of State--certified that Georgia’s election system “can be safely and accurately used by electors at primaries and elections,” as required by Georgia law. O.C.G.A §21-2-379.2. By knowledge and belief, this violates Georgia law because the system has changed since its last certification in 2007--ten years ago.

48.

O.C.G.A §21-2-379.2(b) states that if, upon examination or reexamination the Secretary of State believes “the kind of system so examined can be safely and accurately used by electors at primaries and elections” he shall make and certify a report to that effect and store such a report in his office. O.C.G.A §21-2-379.2(c) states that “No kind of direct recording electronic voting system not so approved shall be used at any primary or election.”

49.

Despite not being certified for use, and despite the pending request for reexamination, Kemp and all Defendants allowed the uncertified and compromised systems to be used in the Runoff.

50.

The right to vote is the foundation of our democracy. It is how we ensure that our government has the consent of the governed. It is enshrined in the Constitution of the United States and in the Constitution of the State of Georgia. Electors have the right to vote, the right to do so by secret ballot, the right to have their ballot accurately tabulated, and the right to be assured that their vote will be counted and recorded accurately. When electors cannot trust that their vote will be accurately counted and recorded, it has a chilling effect and violates those rights. When votes are not properly recorded or counted, then those rights have been violated. In fact, the Georgia Constitution at Article II, Section I, provides the unusual measure of protection for the purity of elections and Georgia electors' rights by incorporating the requirement to comply with all election statutes in the State Constitution.

51.

All of this motivates the present case. The U.S. electoral system has been under attack. Georgia's elections are particularly vulnerable to attack, as the state

uses old, outdated systems with security flaws. Georgia refused help from the DHS to protect its voting systems. Kemp never certified that the system in currently use is safe and accurate—and he has been in office since January 2010. CES was improperly secured, and CES allowed key information to be accessible via the internet—from at least August 2016 until March 2017. After that, the voting system was not forensically tested and analyzed to ensure that it was secure prior to the Special Election or the Runoff.

52.

Electors have constitutional rights to know that their votes will be accurately recorded and tabulated. Given the circumstances under which the Runoff was held, electors who voted using Georgia’s DRE-Based Voting System cannot be certain that their votes were recorded or counted as cast. Consequently, considerable doubt has been cast on the results of the election as a result of the aforementioned irregularities and misconduct of officials.

II. JURISDICTION AND VENUE

53.

Plaintiffs bring claims under the United States Constitution, the Georgia Constitution, and the laws of the State of Georgia. This Court has jurisdiction

based upon O.C.G.A. §§ 9-4-1 to -10 to grant declaratory relief; based upon O.C.G.A. §§ 9-5-1 to -11 to grant injunctive relief; and based upon O.C.G.A. §§ 9-6-20 to -28 to grant relief by way of issuing the writ of mandamus.

54.

Venue in this Court is proper under O.C.G.A. § 9-10-30 because Fulton County is the county of residence of at least one of the Defendants against whom substantial equitable relief is prayed. The principal office of the Secretary of State's Elections Divisions is located at 2 Martin L. King Jr. Drive SE, Suite 1104, Atlanta, Fulton County, Georgia, 30334, as such, jurisdiction and venue are proper in this Court.

III. PLAINTIFFS

55.

Plaintiff DONNA CURLING (“Curling”) is an elector of the State of Georgia and a resident of Fulton County and the 6th Congressional District of the State of Georgia. Curling is a member of the COALITION FOR GOOD GOVERNANCE. Curling is an “aggrieved elector who was entitled to vote” for a candidate in the Runoff under O.C.G.A. § 21-2-521. Furthermore, the ballot system under which she cast her vote substantially burdens her right to vote, as the

system is fundamentally insecure, is illegally employed, and cannot be reasonably relied upon to have properly recorded and counted her vote and the votes of other electors. As such, she has standing to bring her claims.

56.

Plaintiff COALITION FOR GOOD GOVERNANCE. (“CGG”), is a non-profit corporation organized and existing under the laws of the State of Colorado (formerly Rocky Mountain Foundation). CGG’s purpose is to advance the constitutional liberties and individual rights of citizens, with an emphasis on elections, by--among other activities--engaging in and supporting litigation. CGG is a membership organization. Its membership includes Curling, Donna Price (“Price”), and other electors of the State of Georgia who reside in, variously, Fulton County, Cobb County, DeKalb County, and the 6th Congressional District of the State of Georgia. Several of CGG’s Georgia elector members voted in the Runoff.

57.

Plaintiff CGG has associational standing to bring this complaint on behalf of CGG’s Georgia individual elector members because (1) those members would otherwise have standing to sue in their own right; (2) the interests CGG seeks to protect are germane to CGG’s purpose; and because (3) with the exception of

Courts IV and V, the relief requested herein does not require the participation of CGG's individual Georgia elector members in the lawsuit.

58.

Plaintiff DONNA PRICE is an elector of the State of Georgia and a resident of DeKalb County. Price was among the Georgia electors who signed the May 10, 2017 and May 17, 2017 letters requesting that Kemp re-examine the state's voting system. Also, Price casts her ballot under a system which substantially burdens her right to vote, as the system is fundamentally insecure and illegally employed, and cannot be reasonably relied upon to record and count her votes properly and the votes of other voters. As such, she has standing to bring a writ of mandamus claim.

59.

Plaintiff JEFFREY SCHOENBERG ("Schoenberg") is an elector of the State of Georgia and a resident of DeKalb County and the 6th Congressional District of the State of Georgia. Schoenberg is also an "aggrieved elector who was entitled to vote" for a candidate in the Runoff under O.C.G.A. § 21-2-521. Furthermore, the ballot system under which he cast his vote substantially burdens his right to vote, as the system is fundamentally insecure and illegally employed, and cannot be reasonably relied upon to have properly recorded and counted his vote and the votes of other voters. As such, he has standing to bring his claims.

60.

Plaintiff LAURA DIGGES (“L. Digges”) is an elector of the State of Georgia and a resident of Cobb County and the 6th Congressional District of the State of Georgia. L. Digges is also an “aggrieved elector who was entitled to vote” for a candidate in the Runoff under O.C.G.A. § 21-2-521. Furthermore, the ballot system under which she cast her vote substantially burdens her right to vote, as the system is fundamentally insecure and illegally employed, and cannot be reasonably relied upon to have properly recorded and counted her vote and the votes of other voters. As such, she has standing to bring her claims.

61.

Plaintiff WILLIAM DIGGES III (“W. Digges”) is an elector of the State of Georgia and a resident of Cobb County and the 6th Congressional District of the State of Georgia. W. Digges is an “aggrieved elector who was entitled to vote” for a candidate in the Runoff under O.C.G.A. § 21-2-521. Furthermore, the ballot system under which he cast his vote substantially burdens his right to vote, as the system is fundamentally insecure and illegally employed, and cannot be reasonably relied upon to have properly recorded and counted his vote and the votes of other voters. As such, he has standing to bring her claims.

62.

Plaintiff RICARDO DAVIS (“Davis”) is an elector of the State of Georgia and a resident of Cherokee County. Davis was among the Georgia electors who signed the May 10, 2017 and May 17, 2017 letters requesting that Kemp re-examine the state’s voting system. Also, Davis casts his ballot under a system which substantially burdens his right to vote, as the system is fundamentally insecure and illegally employed, and cannot be reasonably relied upon to record and count his votes properly and the votes of other voters. As such, he has standing to bring a writ of mandamus claim.

IV. DEFENDANTS

63.

Defendant BRIAN P. KEMP is the Secretary of State of Georgia and, in that role, is also Chair of the State Election Board. In his official and individual capacity, he is responsible for the orderly and accurate administration of Georgia’s the electoral processes. This responsibility includes the duty to approve the use of Georgia’s voting systems and to conduct any reexaminations of Georgia’s voting systems, upon request or at his own discretion. O.C.G.A. § 21-2-379.2(a)-(b). See O.C.G.A. § 21-2-50.

64.

Defendants DAVID J. WORLEY, REBECCA N. SULLIVAN, RALPH F. “RUSTY” SIMPSON, and SETH HARP (“Members of the State Election Board”) are members of the State Election Board in Georgia. In their individual capacities and their official capacities as members, they are responsible for (1) promulgating rules and regulations to ensure the legality and purity of all elections, (2) investigating frauds and irregularities in elections, and (3) reporting election law violations to the Attorney General or appropriate district attorney. O.C.G.A. § 21-2-31.

65.

Defendant STATE ELECTION BOARD (“State Board”) is responsible for (1) promulgating rules and regulations to ensure the legality and purity of all elections, (2) investigating frauds and irregularities in elections, and (3) reporting election law violations to the Attorney General or appropriate district attorney. O.C.G.A. § 21-2-31.

66.

Defendant RICHARD BARRON (“Barron”) is the Director of the Fulton County Board of Elections and Registration. In his official and individual capacity, he was responsible for conducting the Special Election and the Runoff in Fulton County.

67.

Defendants MARY CAROLE COONEY, VERNETTA NURIDDIN, DAVID J. BURGE, STAN MATARAZZO, and AARON JOHNSON (“Members of Fulton County Board of Registration and Elections”) are members of the Fulton County Board of Registration and Elections. In their official and individual capacities, they were responsible for conducting the Special Election and Runoff in Fulton County.

68.

Defendant FULTON COUNTY BOARD OF ELECTIONS AND REGISTRATION (“Fulton Board”) is responsible for conducting elections in Fulton County, including the Runoff.

69.

Defendant MAXINE DANIELS (“Daniels”) is the Director of Voter Registrations and Elections for DeKalb County. In her official and individual capacity, she is responsible for conducting the elections in DeKalb County, including the Runoff.

70.

Defendants MICHAEL P. COVENY, ANTHONY LEWIS, LEONA PERRY, SAMUEL E. TILLMAN, and BAOKY N. VU (“Members of DeKalb County Board of Registrations and Elections”) are members of the DeKalb County

Board of Registration and Elections. In their official and individual capacities, they were responsible for conducting the Special Election and Runoff in DeKalb County.

71.

Defendant DEKALB COUNTY BOARD OF ELECTIONS AND REGISTRATION (“DeKalb Board”) is responsible for conducting elections in DeKalb County, including the Runoff.

72.

Defendant JANINE EVELER (“Eveler”) is the Director of the Cobb County Board of Elections and Registration. In her official and individual capacity, she is responsible for conducting the elections in Cobb County, including the Runoff.

73.

Defendants PHIL DANIELL, FRED AIKEN, JOE PETTIT, JESSICA BROOKS, and DARRYL O. WILSON (“Cobb County Board of Elections and Registration”) are members of the Cobb County Board of Elections and Registration. In their official and individual capacities, they were responsible for conducting the Special Election and Runoff in Cobb County.

74.

Defendant COBB COUNTY BOARD OF ELECTIONS AND REGISTRATION (“Cobb Board”) is responsible for conducting elections in Cobb County, including the Runoff.

75.

Defendant MERLE KING (“King”) is Executive Director of the Center for Election Systems at Kennesaw State University. In his official and individual capacities, he is responsible for overseeing and maintaining Georgia’s DRE-Based Voting System registration systems used in the Special Election and the Runoff.

76.

Defendant THE CENTER FOR ELECTION SYSTEMS AT KENNESAW STATE UNIVERSITY is responsible for overseeing and maintaining Georgia’s DRE-Based Voting System used in the Special Election and the Runoff.

V. FACTUAL ALLEGATIONS

77.

The allegations of paragraphs 1 through 76 above are hereby incorporated as the allegations of this paragraph 77 in this complaint.

78.

Plaintiffs are electors of the State of Georgia, and an association that includes among its members electors of the State of Georgia, who are concerned about the integrity, credibility, security, and reliability of the electoral process.

79.

Their concern about the integrity, credibility, security, and reliability of the electoral process has led them to oppose the general use of Georgia's unsafe, uncertified, insecure, and inaccurate voting system ("Georgia's direct-recording electronic ('DRE')-Based Voting System"), and specifically its use during the Runoff.

A. GENERAL ALLEGATIONS

80.

On June 20, 2017, the Runoff was held to fill a vacancy left by the previous incumbent, Congressman Tom Price. Advance voting in the Runoff began on May 30, 2017, pursuant to O.C.G.A. § 21-2-385(d). On June 26, 2017 Karen Handel was certified as the winner of the election.²⁵ ²⁶

²⁵ Kemp Certifies June 20 Runoff, Office of the Secretary of State of the State of Georgia, June 27, 2017, http://sos.ga.gov/index.php/general/kemp_certifies_june_20_runoff (last visited July 3, 2017)

81.

Georgia's 6th Congressional District spans portions of Fulton, Cobb, and DeKalb counties.

82.

O.C.G.A. § 21-2-379.2(c) prohibits the use, in any primary or election, of any kind of DRE voting system not approved by the Secretary of State at any primary or election.

83.

Georgia's DRE-Based Voting System, as currently in use in all 159 of Georgia's counties consists of the following configuration of components and related firmware and software:

- Optical Scan: AccuVote OS 1.94W
- Touch Screen: R6 – Ballot Station 4.5.2! and TSx – Ballot Station 4.5.2!

²⁶ O.C.G.A. § 21-2-524 requires that “A petition to contest the result of a primary or election shall be [...] within five days after the official consolidation of the returns of that particular office or question and certification thereof by the election official having responsibility for taking such action under this chapter.” This would place the filing deadline on Saturday July 1, 2017. O.C.G.A. § 1-3-1(c) states “when a period of time measured in days, weeks, months, years, or other measurements of time except hours is prescribed for the exercise of any privilege or the discharge of any duty, the first day shall not be counted but the last day shall be counted; and, if the last day falls on Saturday or Sunday, the party having such privilege or duty shall have through the following Monday to exercise the privilege or to discharge the duty.” Thus the deadline for filing a challenge to the Runoff is July 3, 2017.

- ExpressPoll: ExpressPoll 4000 and 5000 running software; Easy Roster; 2.1.2 and Security Key 4.5+
- Election Management System: GEMS 1.18.22G!
- Honeywell barcode scanner: MK1690-38-12-IFI, used with ExpressPoll pollbooks

(Together, the foregoing will be known as “Georgia’s DRE-Based Voting System”). There is no evidence that any Secretary of State ever approved of or certified the system as safe and accurate in its current form.

84.

Defendant Barron and the Fulton Board used Georgia’s DRE-Based Voting System to conduct the Special Election and Runoff in Fulton County.

85.

Defendant Daniels and the DeKalb Board used Georgia’s DRE-Based Voting System to conduct the Special Election and Runoff in DeKalb County.

86.

Defendant Eveler and the Cobb Board used Georgia’s DRE-Based Voting System to conduct the Special Election and Runoff in Cobb County.

87.

O.C.G.A. § 21-2-379.2(a) grants to any ten or more concerned electors the right to require the Secretary of State “at any time” to conduct a reexamination of a

previously examined and approved DRE voting system. Specifically, O.C.G.A. § 21-2-379.2(a) reads as follows:

(a) Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any direct recording electronic voting system may request the Secretary of State to examine the system. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any such system previously examined and approved by him or her. Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination. The Secretary of State may, at any time, in his or her discretion, reexamine any such system.

The clear intent of the statute is to permit a timely re-examination of a voting system in question prior to a pending election.

88.

O.C.G.A. § 21-2-379.2(b) provides that, upon receiving such a request for reexamination from ten or more electors, the Secretary of State has a duty to reexamine the DRE voting system. The statute reads as follows:

(b) The Secretary of State shall thereupon examine or reexamine such direct recording electronic voting system and shall make and file in his or her

office a report, attested by his or her signature and the seal of his or her office, stating whether, in his or her opinion, the kind of system so examined can be safely and accurately used by electors at primaries and elections as provided in this chapter. If this report states that the system can be so used, the system shall be deemed approved; and systems of its kind may be adopted for use at primaries and elections as provided in this chapter.

89.

O.C.G.A. § 21-2-379.2(c) provides that, if reexamination shows that a DRE voting system “can no longer be safely or accurately used” then the approval of that system “shall immediately be revoked by the Secretary of State; and no such system shall thereafter ... be used in this state.” (emphasis added). The statute reads as follows:

(c) No kind of direct recording electronic voting system not so approved shall be used at any primary or election and if, upon the reexamination of any such system previously approved, it shall appear that the system so reexamined can no longer be safely or accurately used by electors at primaries or elections as provided in this chapter because of any problem concerning its ability to accurately record or tabulate votes, the approval of the same shall immediately be revoked by the Secretary of State; and no

such system shall thereafter be purchased for use or be used in this state.
(emphasis added).

90.

Georgia's election laws contemplate that elections normally required to be conducted using voting equipment may instead be conducted using paper ballots if circumstances so require.

91.

First, O.C.G.A. § 21-2-334 provides as follows:

§ 21-2-334. Voting by ballot

If a method of nomination or election for any candidate or office, or of voting on any question is prescribed by law, in which the use of voting machines is not possible or practicable, or in case, at any primary or election, the number of candidates seeking nomination or nominated for any office renders the use of voting machines for such office at such primary or election impracticable, or if, for any other reason, at any primary or election the use of voting machines wholly or in part is not practicable, the superintendent may arrange to have the voting for such candidates or offices or for such questions conducted by paper ballots. In such cases, paper ballots shall be printed for such candidates, offices, or questions, and the primary or

election shall be conducted by the poll officers, and the ballots shall be counted and return thereof made in the manner required by law for such nominations, offices, or questions, insofar as paper ballots are used.

92.

Second, O.C.G.A. § 21-2-281 provides as follows:

§ 21-2-281. Use of paper ballots where use of voting equipment impossible or impracticable

In any primary or election in which the use of voting equipment is impossible or impracticable, for the reasons set out in Code Section 21-2-334, the primary or election may be conducted by paper ballot in the manner provided in Code Section 21-2-334.

93.

Third, O.C.G.A. § 21-2, Article 11, Part 2, provides the detailed procedures that are required to be used in precincts that conduct primaries and elections using paper ballots.

B. KNOWN SECURITY AND ACCURACY PROBLEMS IN GEORGIA'S DRE-BASED VOTING SYSTEM

94.

Georgia's DRE-Based Voting System is subject to widely known safety and accuracy concerns as summarized in the affidavits of Professor Duncan Buell and Professor Edward Felten. Affidavit of Duncan Buell, attached as "Exhibit G" and Exhibit E, respectively.

95.

In considering the use of Georgia's DRE-Based Voting System, its inherent deficiencies and recent security failures must be acknowledged. These inherent deficiencies and recent security failures include, but are not limited to:

96.

First, the legal--but still troubling--infiltration of Georgia's DRE-Based Voting System via CES's public webpage by Lamb in August 2016 and again in March 2017 by Grayson. See Exhibit A.

97.

Second, numerous critical security vulnerabilities and deficiencies were identified prior to the Special Election and Runoff at CES. CES is responsible for ensuring the integrity of the voting systems and developing and implementing security procedures for the election management software installed in all county election offices and voting systems. CES also is responsible for programming these systems for each election, and providing all counties with instructions for accessing the system's software. A security breach at CES could have dire security

consequences for the integrity of the technology used for elections in Georgia. CES's security and cybersecurity was reviewed at a high level "walkthrough" review by KSU UITS Information Security Office. See Exhibit C. This walkthrough discovered several immediately obvious security vulnerabilities were reported in an incident report. Exhibit C, pages 2-4.

98.

Third, on May 24, 2017, after becoming aware of problems with the electronic tabulation of the votes cast in Fulton County in the Special Election, sixteen computer scientists wrote Defendant Kemp to express profound concerns about the lack of verifiability and unacceptable security of Georgia's DRE-Based Voting System. Letter from various experts to Brian Kemp, Secretary of State, May 24, 2015 Attached as "Exhibit H". The computer scientists reiterated cybersecurity concerns that many of them had expressed in a similar letter sent on March 15, 2017, following the remote electronic intrusion into the Georgia's system in March 2017. Letter from various experts to Brian Kemp, Secretary of State, March 15, 2017 Attached as "Exhibit I", pages 1-2. The computer scientists urged Defendant Kemp to treat the breach at CES "as a national security issue with all seriousness and intensity." Exhibit H, at 1. They stated that "a truly comprehensive, thorough and meaningful forensic computer security investigation likely would not be completed in just a few weeks." Id. They warned that the error

that occurred in Fulton County during the Special Election could indicate a corrupted database that must be investigated. The computer scientists urged the use of paper ballots. Id. at 2.

99.

Fourth, failures in Georgia's DRE-Based Voting System caused improper memory cards to be uploaded into the election database during the Special Election. Upon information and belief, Defendant Barron told the Fulton County Board of Commissioners that the system did not prevent the uploading of improper election memory cards and data and only generated an unintelligible error message when an attempt was made to export the results from the Global Election Management System ("GEMS") into the Election-Night Reporting system (a separate internet-based application to report results to the public). Federal voting system standards require controls that prevent the introduction of improper memory cards. Unconventional procedures, including deleting precinct voting results in the database, reportedly were used to correct this error, but the purported corrections themselves lacked a verifiable audit trail. It was reported in the press that Kemp initiated an investigation of the April 18 Fulton County system failure.²⁷ On information and belief, that investigation has not been completed.

²⁷ Aaron Diamant and Berndt Petersen, State Opens Investigation into Issues With 6th District Race, WSBTV, May 26, 2017, <http://www.wsbtv.com/news/local/atlanta/state-opens-investigation-into-issues-with-6th-district-race/514213222> (last accessed June 30, 2017)

100.

Fifth, on all election nights, Fulton County transmits ballot data from touchscreen machine memory cards to the GEMS tabulation server (i.e., the Global Election Management System used in Georgia's DRE-Based Voting System) via modem in an unauthorized configuration that, on information and belief, does not use adequate encryption. Voting system standards that are established by the state require that security of data transmission be assured. The lack of security in electronic transmission exposes the system to, and invites attack.

101.

Seventh, the physical security of DRE voting equipment used in Georgia's DRE Based Voting System has been inadequate during pre- and post-election machine storage, leaving the machines vulnerable to attack and compromise.

102.

Seventh, upon information and belief, Georgia's DRE-Based Voting System does not meet minimum standards, including mandatory audit capacity standards, required by the Help America Vote Act, 52 U.S.C. § 21081.

103.

Eighth, The DRE voting equipment used in Georgia's DRE-Based Voting System provides no audit trail or verifiable record that can be used to recover from a malicious attack, human error, or software failure. Any such failure is difficult or

impossible to detect--unlike errors in a paper ballot system, where problems can be isolated and manually corrected to reflect the voter's intent.

104.

Ninth, there are additional significant security and accuracy concerns that precluded Georgia's DRE-Based Voting System from being used safely and accurately in the June 20 election. See Exhibits A, C, E, and G.

105.

Ninth, Georgia's DRE-Based Voting System is fifteen years old, relies upon a back-end database that is outdated, inadequate, and runs on an operating system that is currently past its support life. Such a relatively old configuration is inherently vulnerable to hacking, errors, and other mischief.

C. DEFENDANT KEMP FAILED TO EXAMINE AND APPROVE THE VOTING SYSTEM

106.

The Secretary of State is required by O.C.G.A. § 21-2-379.2 to formally approve a voting system that can be "safely and accurately used." No such documentation exists for the DRE-based system used in recent years. Elections in Georgia cannot be legally conducted on a system that is not approved as safe and accurate by the Secretary of State.

107.

Any new the Voting system deployed after April 17, 2005 is required to meet the certification standards in Ga. Comp. R. & Regs. 590-8-1-.01. That regulation requires compliance with the most recent Election Assistance Commission (EAC) voting standards. Upon information and belief, Kemp has not attempted to certify the system in use to those mandatory state standards, nor has he certified that it does meet those standards although the current equipment configuration constitutes a new system deployed after April 17, 2005.

108.

On May 10, 2017, a group of Georgia electors including Plaintiff Davis, concerned about the security issues that had become public knowledge, filed a formal request with Secretary Kemp seeking a re-examination of the equipment under the provisions of O.C.G.A. § 21-2-379.2(a). No answer was received until after the electors filed suit against Secretary of State Kemp over his lack of response. See Curling v. Kemp, Case No. 2017CV290630. Upon information and belief Kemp failed to conduct a timely review of the system either at his own initiation or in response to the request of the concerned citizens.

D. IMPROPER CERTIFICATION OF THE ELECTION RESULTS

109.

As noted above, Georgia's DRE-Based Voting System, used for the June 20 election has not been approved in compliance with the election code and regulations, and its use renders an election illegal and unconstitutional under the provisions of the Georgia State Constitution.

110.

To provide for election transparency citizen oversight of Georgia elections, Georgia election regulations, provide for citizen initiated re-canvassing of any precincts which seem to have erroneous results from the DRE-voting machines. Ga. Comp. R. & Regs. 183-1-12. These regulations permit citizens to choose any or all precincts to demand re-canvassing of the votes, by having the memory cards reread by the tabulation server and conducted by the election officials prior to the county-level certification of results. Members of CGG (then Rocky Mountain Foundation) and other citizens wrote to Fulton County, DeKalb County and Cobb County Defendant boards of elections prior to county-level certification specifying the precincts they believe may contain erroneous results, and requesting a canvassing prior to the certification. See Letters to the Defendant DeKalb and Cobb County Election Boards by various electors attached as "Exhibit J". Upon information and belief, a similar letter was also sent to the Fulton County Elections Board. In each case, Defendant county officials denied their properly submitted requests for canvassing.

111.

Prior to each county election board meeting, on behalf of its members who are eligible electors in the 6th Congressional District, CGG filed a letter requesting that each county board deny certification of the election because of the numerous violations of law occurring during the conduct of the election. Letters to the Defendant County Election Boards by CGG (then Rocky Mountain Foundation) attached as “Exhibit K.” The letter and concerns expressed, upon information and belief, were not discussed at any of the county board meetings. The boards simply rubberstamped the results without concern about the legality or accuracy of the returns.

112.

On information and belief, Secretary Kemp almost immediately certified the consolidated return for the Runoff after the DeKalb County certification had taken place, despite the fact that he was informed the Boards had violated electors’ rights to seek a canvass of precincts that appeared to show irregularities or questionable results.

E. Irreparable Harm / Inadequate Remedy at Law

113.

Georgia electors who cast their votes in person during the Runoff-were required to cast their votes using Georgia’s DRE-Based Voting System.

114.

Georgia’s DRE-Based Voting System could not be used safely and accurately by electors voting in the Runoff because Georgia’s DRE-Based Voting System is demonstrably vulnerable to undetectable malfunctions and malicious manipulation that cannot be corrected on a timely or reasonable basis

115.

Each Plaintiff and the Georgia elector members of Plaintiff CGG were harmed in the exercise of their constitutional fundamental right to vote in the Runoff because Georgia used an unsafe, unsecure, and uncertified DRE-Based Voting System that was subjected to undetected, unauthorized access and potential manipulation.

116.

Plaintiffs and the Georgia elector members of Plaintiff CGG cannot be adequately compensated for these harms in an action at law for money damages.

VI. COUNTS

**COUNT I: VIOLATION OF ARTICLE II, SECTION I, PARAGRAPH I, OF
THE GEORGIA CONSTITUTION OF 1983**

**(All Plaintiffs, Against All Defendants In Individual Capacities, Except State
Board, Fulton Board, DeKalb Board, Cobb Board, and CES)**

**Declaratory and Injunctive Relief
O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3**

Enjoining Use of Georgia's DRE-Based Voting System

117.

The allegation of paragraphs 1 through 116 above are hereby incorporated as the allegations of this paragraph 117 of Count One of this complaint.

118.

Article II, Section 1, Paragraph 1 of the Georgia Constitution provides, "Elections by the people shall be by secret ballot and shall be conducted in accordance with procedures provided by law."

119.

Elections must be conducted in accordance the statutes and regulations of the State of Georgia.

120.

The Runoff was not conducted in accordance with the “procedures provided by law” because the DRE-Based Voting System was in violation of O.C.G.A. § 21-2-379.1(8) at the time of the Runoff. O.C.G.A. § 21-2-379.1(8) provides that DRE-Based Voting Systems “shall, when properly operated [by an elector], register or record correctly and accurately every vote cast.”

121.

Georgia’s DRE-Based Voting System violated O.C.G.A. § 21-2-379.1(8) during the Runoff because as a likely compromised system, it cannot be trusted to “record correctly and accurately every vote cast,” even when “properly operated” by electors. Defendants knew that the system had been unsecured, breached and compromised and could not be presumed to be safe or in compliance with statute and governing regulations.

122.

Additionally, the Runoff was not conducted in accordance with the “procedures provided by law” because the DRE-Based Voting System used was in violation of O.C.G.A. § 21-2-379.2. O.C.G.A 21-2-379.2(a) requires the Secretary of State to reexamine the voting system, if “[a]ny ten or more electors of this state request the Secretary of State to reexamine any such system previously examined and approved by him or her.” Id.

123.

That was not done here. Ten Georgia electors requested Kemp re-examine the DRE-Based Voting System prior to the Runoff on four separate occasions: on May 10, 17, and 19, and June 2, 2017. Secretary Kemp’s office responded to the request on June 5, 2017, stating that re-examining the system would cost \$10,000 and take six months. Exhibit D. Declining to reexamine Georgia’s DRE-Based Voting System prior to the Runoff or any currently scheduled 2017 elections.

124.

After a request to examine or reexamine a DRE-based voting system, “no kind of [DRE] voting system” not so examined or reexamined “shall be used at any primary or election.” O.C.G.A. § 21-2-379.2(c). Despite this, the DRE-Based Voting System was used during the Runoff. Kemp was, or should have been, aware that the system security had been compromised and for numerous reasons could not pass certification standards nor be approved as “safe or accurate.” By choosing to move forward, he abrogated his statutory duties and abused his discretion.

125.

The importance of examining and reexamining a DRE-voting system prior to elections is stressed in the Georgia Code. Upon examination, should it “appear that the system... can no longer be safely or accurately used by electors” as

provided under the Georgia Code “because of any problem concerning its ability to accurately record or tabulate votes” then the Secretary of State should “immediately” revoke his approval. O.C.G.A. §21-2-379.2(c). Indeed, given the knowledge Kemp and other Defendants had of how noncompliant and insecure the system was, Defendants had the duty to act to sideline the compromised system even before the electors requested system re-examination.

126.

Since all Defendants individually and collectively did not act to ensure the Runoff complied with the “procedures provided by law,” as alleged above, they have violated the Georgia Constitution

127.

Georgia’s DRE-Based Voting System, as alleged throughout this complaint, cannot be safely and accurately used, nor was it used in the Special Election or Runoff in accordance with the Georgia Constitution or Georgia law.

128.

Accordingly, pursuant to O.C.G.A. § 9-4-2, Plaintiffs pray that this court will declare that these Defendants have violated the Constitution. Pursuant to O.C.G.A. § 9-4-3, Plaintiffs also pray that this court will enjoin Defendants to void the election because accurate results tabulated in accordance with Georgia law

cannot be determined. This court should also enjoin Defendants' use of Georgia's DRE-Based Voting System for future elections.

COUNT II: VIOLATION OF 42 USC § 1983 – DUE PROCESS

(All Plaintiffs, Against All Defendants In Official Capacities Except State Board, Fulton Board, DeKalb Board, Cobb Board, and CES)

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

42 USC § 1983

129.

The allegations of paragraphs 1 through 128 above are hereby incorporated as the allegations of this paragraph 129 of Count Two of this complaint.

130.

42 U.S.C. § 1983 provides that “[e]very person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any

rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress . . .”

131.

The failure to comply with the Georgia Constitution and the Georgia Code concerning elections is a violation of federal due process when the patent and fundamental fairness of the election is called into question.

132.

Patent and fundamental fairness of an election is called into question when allegations go well beyond an ordinary dispute over the counting and marking of ballots. Such is the case here.

133.

Elected Georgia government officials—and those they control—denied the electorate the right granted by Georgia Constitution to choose their elected official in accordance with the procedures provided by state law. Ga. Const. art. II, § 1, ¶ 2. These state officials include Defendants Kemp, Members of the State Board, Barron, Members of the Fulton Board, Daniels, Members of the DeKalb Board, Eveler, members of the Cobb Board, and King.

134.

Defendants violated O.C.G.A. § 21-2-379.1(8) which provides that any DRE system used in Georgia must, when properly operated by the elector, “record correctly and accurately every vote cast.” Consistent with experts who state that Georgia’s DRE-Based Voting System must be presumed to have been compromised, it is more than probable that Georgia’s DRE-Based Voting System was compromised prior to the Runoff and that the system could not correctly or accurately count every vote during the Runoff. As a result, the tabulation of the voters’ intent cannot reasonably be known.

135.

Instead, despite receiving multiple warnings that the DRE-Based Voting System had been compromised--and knowing that documents capable of enabling a malicious attack were accessed and downloaded at least twice from the CES without authorization--Kemp responded by stating that the system was secure and that no review was needed. These actions amount to a purposeful and willful substantial burdening of the fundamental right to vote.

136.

Additionally, Georgia’s DRE-Based Voting System must be properly certified, reexamined, and approved by the Secretary of State prior to any election, when so requested by ten or more electors. O.C.G.A. § 21-2-379.2; See Ga Comp.

R. & Regs. 590-8-1.01. Here, the Secretary of State did not certify, reexamine or approve the system. See Counts VII and VIII, respectively.

137.

By violating the Georgia Constitution, Georgia's election officials distributed to electors in Georgia's 6th Congressional District an illegal ballot, precluding their right to vote on a legal ballot in the Runoff. See Counts Count IV and V, respectively.

138.

Under the circumstances alleged above, relief under 42 U.S.C. § 1983 is warranted. Accordingly, Plaintiffs ask this Court to declare that these Defendants have violated the fundamental right to due process of Plaintiffs and enjoin Defendants to void the election. This court should also enjoin Defendants' use of Georgia's DRE-Based Voting System for future elections.

COUNT III: VIOLATION OF 42 USC § 1983 – EQUAL PROTECTION

(All Plaintiffs, Against All Defendants In Official Capacities, Except State Board, Fulton Board, DeKalb Board, Cobb Board, and CES)

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

42 USC § 1983

139.

The allegations of paragraphs 1 through 138 above are hereby incorporated as the allegations of this paragraph 139 of Count Three of this complaint.

140.

42 U.S.C. § 1983 provides that “[e]very person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress”

141.

The Equal Protection Clause of the Fourteenth Amendment mandates that “[n]o State shall . . . deny to any person within its jurisdiction the equal protection of the laws.” U.S. Const. amend. XIV § 1.

142.

The Plaintiffs are all similarly situated to other registered electors in the Runoff who voted by paper ballot.

143.

The Secretary of State and Election Boards allowed electors using a paper ballot to vote in the Runoff to vote using properly verifiable, recountable ballots. These ballots are properly verifiable and recountable to the extent that they can be counted manually, rather than counted electronically, in a manner necessarily exposed to irregularity. Such paper ballots could be hand counted and reviewed for verification by the court in the proceedings of this contest, although electronic ballots cannot be verified in such a contest. The voters of the respective ballots have their votes unequally weighted, with favorable treatment given to those who voted by paper ballot.

144.

Comparatively, all Defendants forced electors using the DRE voting system in the Runoff to vote using illegal and improperly certified ballots that cannot be reviewed by the court in this election contest. These include Kemp, Members of the State Board, Barron, Members of the Fulton Board, Daniels, Members of the DeKalb Board, Eveler, members of the Cobb Board, and King.

145.

Again, despite receiving warning that the DRE-Based Voting System had been compromised—and knowing that documents capable of enabling a malicious attack were accessed and downloaded from the CES at least twice without authorization—the Secretary of State responded by publicly repeatedly stating that the system was secure and no review was needed. He also did so in the face of overwhelming and repeated warnings from experts that the system must be presumed to have been compromised, and that the results could not be considered reliable. These actions by all Defendants amount to purpose and willful substantial burdening of the right to vote.

146.

The electors who voted by paper ballot were able to vote in the election using properly verifiable, recountable ballots, which can be counted and reviewed under the supervision of this Court, while voters using the DRE system are not reviewable—thus creating two classes of electors.

147.

The use of illegal and improperly constructed ballots in Georgia’s DRE-Based Voting System severely infringed upon the Plaintiffs’ fundamental right to vote by not providing the opportunity to cast a lawful vote in accordance with the Georgia Constitution or code.

148.

The burdens and infringements imposed upon these fundamental rights were differentially imposed upon paper ballot voters and DRE system voters during the Runoff without justification by any substantial or compelling state interest that could not have been accomplished by other, less restrictive means. As the United States Supreme Court has noted, “The right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another.” Bush v. Gore, 531 U.S. 98, 104-105 (2000) (citing Harper v. Virginia Bd. of Elections, 383 U.S. 663, 665 (1966) (“[O]nce the franchise is granted to the electorate, lines may not be drawn which are inconsistent with the Equal Protection Clause of the Fourteenth Amendment.”). The Supreme Court continued, “It must be remembered that ‘the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise.’” Id. (quoting Reynolds v. Sims, 377 U.S. 533, 555 (1964)).

149.

Even under a rational basis standard, there is no rational basis for unequal treatment of electors predicated on actions in violation of the Georgia Constitution and Code.

150.

Defendant's conduct described herein violated the Fourteenth Amendment right of the Plaintiffs to enjoy equal protection of the law.

151.

Under the circumstances alleged above, relief under 42 U.S.C. § 1983 is warranted. Defendants showed purposeful and intentional disregard for the fundamental and wholesale problems of the DRE-Based Voting System by not reexamining the system, because they willfully, despite overwhelming evidence to the contrary, refused to act on the fact that there were significant security threats against Georgia's non-compliant DRE-Based Voting System.

152.

Plaintiffs ask this Court to declare that these Defendants have violated the fundamental right to equal protection of Plaintiffs and enjoin Defendants to void the Runoff election, and declare a new election to be held as the only just relief available under the laws of Georgia. Plaintiffs ask the Court to prohibit the use of Georgia's DRE-Based Voting System in future elections.

**COUNT IV: ELECTION CONTEST DUE TO MISCONDUCT AND
IRREGULARITY -- USE OF UNSECURE UNCERTIFIED DRE-BASED
VOTING SYSTEM**

**(By all Plaintiffs, except Price, Davis, and CGG, against all Defendants in
their Official and Individual Capacities, except King and CES)**

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

O.C.G.A. § 21-2-520

153.

The allegations of paragraphs 1 through 152 above are hereby incorporated as the allegations of this paragraph 153 of Count Four of this complaint.

154.

Under O.C.G.A. § 21-2-520, a Contestant is entitled to “contest the result of any primary or election.”

155.

A Contestant can be “any aggrieved elector who was entitled to vote” in an election. O.C.G.A. § 21-2-520. Plaintiffs Curling, L. Diggs, B. Diggs, and Schoenberg were all aggrieved electors in the Runoff. On June 26, 2017, Karen Handel was certified as the winner of the Runoff.

156.

An aggrieved elector has the right to contest the election by naming as a defendant in a lawsuit the “election superintendent or superintendents who conducted the contested primary or election.” O.C.G.A. § 21-2-520(c). Election superintendents include either “the county board of elections [or] the county board of elections and registration” as the case may be. O.C.G.A. § 21-2-2(35)(a) Additionally, it can include the Secretary of State. See Dawkins-Haigler v. Anderson, 799 S.E.2d 180 (2017). Here, Plaintiffs named such appropriate defendants.

157.

Since Boards and their members are “superintendents” under the meaning of this statute (including the State Board), by statute, the Defendants State Board, Fulton Board, DeKalb Board, Cobb Board, as well as their respective individual members, including Kemp as Chair of the State Board lack immunity to an election contest claim. See O.C.G.A. § 21-2-520.

158.

The result of any election may be contested if, among other reasons, there is “misconduct, fraud, or irregularity” on the part of any “election official or officials sufficient to change or place in doubt the result.” O.C.G.A. § 21-2-522(1).

159.

Here, the use of Georgia’s DRE-based voting system, given its lack of required certification, compromised security, non-compliance with the election code, and unverifiability of the system, amounts to an “irregularity” that, at a minimum, “place[s] in doubt” the result of this election. O.C.G.A. § 21-2-522(1).

160.

Georgia’s DRE-Based Voting System, approved for use in the Runoff by “election official or officials,” compromised the votes of approximately 232,712 electors. 232,712 votes are significantly greater than the purported margin of victory in the Runoff – 9,702. Therefore, the certified results of the election are placed in significant doubt.

161.

Accordingly, Plaintiffs file this petition to contest the Runoff election results, in addition to their other claims herein. Plaintiffs pray this court declare this election void *ab initio* the election and declare a new election to be held as the only just relief available under the laws of Georgia.

**COUNT V - ELECTION CONTEST DUE TO IRREGULARITY -- USE OF
ILLEGAL BALLOTS**

**(By all Plaintiffs, except Price, Davis and CGG, against all Defendants in their
Official and Individual Capacities, except King and CES)**

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

O.C.G.A. § 21-2-520

162.

The allegations of paragraphs 1 through 161 above are hereby incorporated as the allegations of this paragraph 162 of Count Five of this complaint.

163.

Electors in the Runoff who used Georgia's DRE-Based Voting System to cast their vote used illegal ballots. Illegal ballots are an "irregularity" by "an election official or officials." O.C.G.A. § 21-2-522(1); See Mead v. Sheffield, 278 Ga 268, 270 (2004).

164.

When illegal ballots are used, how electors voted on the illegal ballots is irrelevant.

165.

Instead, the question is whether the number of illegal ballots use is “sufficient to change or place in doubt the result” of the election. The number of illegal ballots is sufficient enough to change or place in doubt the result of the election when the amount used by electors to cast their votes is greater than the margin of victory. See Mead v. Sheffield, 278 Ga. 268, 270 (2004).

166.

In the Runoff, 260,455 ballots were cast. Of those ballots, approximately 232,712 were cast using the DRE system. The remaining 27,742 votes were cast by paper ballot. 232,712 is significantly greater than the margin of victory in the Runoff – 9,702. The paper ballots were also improperly counted through electronic means, although they can be recounted by verifiable means in this proceeding. Given the extensive use of illegal ballots, the results of the election are placed in substantial doubt.

167.

The DRE ballots used in the Runoff were illegal because they did not adhere to the Georgia Constitution or Code. When a ballot does not follow a mandate from the Georgia Constitution or the Georgia Code the ballot is “illegal.” See Mead v. Sheffield, 278 Ga. 268, 269 (2004).

168.

Defendants State Board, Fulton Board, DeKalb Board, Cobb Board, as well as their respective individual members, including Kemp as Chair of the State Board bear statutory responsibility, as “superintendents,” for allowing illegal ballots to proceed under the DRE-based system. See O.C.G.A. § 21-2-520. They do not have immunity to this claim.

169.

Since the Runoff used illegal ballots in sufficient number to place the election in doubt, Plaintiffs file this petition to contest the Runoff election results, in addition to their other claims herein. Plaintiffs pray this court declare the Runoff election *void ab initio*.

COUNT VI: FAILURE TO RECANVASS VOTES

(Plaintiff CGG Against Defendants Kemp, State Board, Barron, Members of the Fulton Board, Daniels, Members of the DeKalb Board, Eveler, Members of the Cobb Board, in their Official and Individual Capacities)

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3

Ga. Comp. R. & Regs. 183-1-12

170.

The allegations of paragraphs 1 through 169 above are hereby incorporated as the allegations of this paragraph 170 of Count Six of this complaint.

171.

Georgia law states: “The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made.” Ga. Comp. R. & Regs. 183-1-12-.02(7)(a).

172.

For the reasons alleged above, Georgia’s DRE-Based Voting System must be assumed to have caused substantial discrepancies or errors in returns, even if not apparent on the literal face of the returns.

173.

Plaintiff CGG includes members that petitioned the DeKalb Board and the Cobb Board to recanvass certain precincts in both counties. See Exhibit J. Upon information and belief members of Plaintiff CGG also sent such a letter to the Fulton County Board. The precincts in which recanvassing was sought, were

selected based on anomalous appearing results including extreme swings between absentee mail in paper ballot voting results and election day results for votes cast using Georgia's DRE Based Voting System.

174.

Defendants Barron, Members of the Fulton Board, Daniels, Members of the DeKalb Board, Eveler, and Members of the Cobb Board refused to recanvass these precincts. Kemp's office was notified of the Fulton BoE's violation of electors' rights on the morning of June 26, hours prior to his decision to certify the results of the election. He chose not to remedy the Fulton BoE's violation by ordering a recanvass of the requested precincts, and ignored the properly filed request. This action represents willful misconduct by Kemp.

175.

Defendants violated their duty under Ga. Comp. R. & Regs. 183-1-12. Concurrently, they violated the citizen's right of oversight and review.

176.

Plaintiffs pray this court declare that Defendants are in violation of their duty to recanvass these precincts. Plaintiffs also pray that this court will enjoin Defendants to void their respective certification of election results, and Kemp to void the certification of the consolidated returns.

**COUNT VII: LACK OF CERTIFICATION OF DRE-BASED VOTING
SYSTEM**

(All Plaintiffs, Against Defendant Kemp, in His Individual Capacity)

Declaratory and Injunctive Relief

O.C.G.A. § 9-4-2 and O.C.G.A. § 9-4-3 and § 21-2-379.2

Ga. Comp. R. & Regs. 590-8-1-.01

177.

The allegation of paragraphs 1 through 176 above are hereby incorporated as the allegations of this paragraph 177 of Count Seven of this complaint.

178.

Under Georgia law, the Secretary of State is responsible for approving Georgia's voting systems as safe and accurate under the provisions of § 21-2-379.2 and certifying Georgia's voting systems under Ga. Comp. R. & Regs. 590-8-1-.01(d)(7.) The purpose of the certification process is to ensure that "hardware, firmware, and software have been shown to be reliable, accurate, and capable of secure operation before they are used in elections in the state." Id. at (a)(3).

179.

Certification by the Secretary of State is not required on systems implemented before April 17, 2005, unless there has been “a modification to the hardware, firmware, or software of the voting system.” Id. At (b)(4). In such a case, under Georgia regulations, the previous State certification becomes invalid.

180.

Upon information and belief, unlike his predecessors—former Secretary Cox and former Secretary Handel—Kemp has not tested Georgia’s DRE-Based Voting System in its current configuration although significant changes to the system have been implemented since the most recent certification. Moreover, he has not certified the DRE-Based Voting System in its current form.

181.

The system configuration was last certified in November 2007 by then Secretary Handel. Since various components have been added and modified since, without required new system certification, the system in use is not properly certified.

182.

Kemp, by law, must certify any new system configuration, tested as an integrated whole, before it can be used in any election. He has not. Georgia’s DRE-Based Voting Systems during the Special Election and Runoff were, therefore,

illegal. Kemp, upon information and belief, intends to keep using these uncertified systems.

183.

Moreover, Plaintiff CGG (then-named Rocky Mountain Foundation) along with multiple Georgia electors inquired about the certification of the system. See Exhibit D. This resulted in an invitation to examine the certifications kept on file in the Secretary of States' Office. Id. A review of that file showed that no certification existed for Georgia's current DRE-system. See Exhibit F.

184.

Accordingly, pursuant to O.C.G.A. § 9-4-2, Plaintiffs pray that this court will declare that these Kemp has not certified or approved the DRE-Based Voting System in its present form, a violation of Georgia law. Pursuant to O.C.G.A. § 9-4-3, Plaintiffs also pray that this court will enjoin Defendants' use of Georgia's DRE-Based Voting System.

COUNT VIII: WRIT OF MANDAMUS

**(All Plaintiffs, Except Laura Digges, William Digges III, and Schoenberg,
Against Defendant Kemp, in His Individual Capacity)**

Writ of Mandamus

O.C.G.A. § 9-4-3 and O.C.G.A. § 9-4-2; O.C.G.A. § 9-6-20

Requiring Exercise of the Public Duty to Reexamine Georgia's DRE-Based Voting System Established By O.C.G.A. § 21-2-379.2(b)

185.

The allegation of paragraphs 1 through 184 above are hereby incorporated as the allegations of this paragraph 185 of Count Eight of this complaint.

186.

Mandamus is a remedy for “government[al] inaction—the failure of a public official to perform a clear legal duty.” Southern LNG, Inc. v. MacGinnitie, 294 Ga. 657, 661 (2014).

187.

Mandamus is warranted when (1) a public official has a clear legal duty to perform an official act (as requested); (2) that the requesting party has a clear legal right to the relief sought or that the public official has committed a gross abuse of discretion; and (3) that there is no other adequate legal remedy. See Bland Farms, LLC v. Georgia Dept. of Agriculture, 281 Ga. 192, 193 (2006); see also SJN Props., LLC v. Fulton County Bd. of Assessors, 296 Ga. 793, 800 (2015); Trip Network, Inc. v. Dempsey, 293 Ga. 520, 522 (2013); Goldman v. Johnson, 297 Ga. 115, 116 (2015).

188.

The Georgia General Assembly has the power to determine the Secretary of State's clear legal duties. See Ga Const. art. 5, § 3, ¶ III ("[T]he General Assembly shall prescribe the powers, duties, compensation, and allowances of... executive officers..."). The General Assembly did so under O.C.G.A. § 21-2-50, which requires the Secretary of State to "perform such other duties as may be prescribed by law."

189.

One clear duty of the Secretary of State, as prescribed by law, is that "the Secretary of State may, at any time, in his or her discretion, reexamine any DRE-based system." O.C.G.A. § 21-2-379.2(a). The clear purpose Secretary of State's power to reexamine any DRE-based system at his discretion is to ensure that the DRE-system can be "safely and accurately used by electors at primaries and elections." O.C.G.A. § 21-2-379.2(b).

190.

Defendant Kemp abused his discretion by not reexamining Georgia's DRE-Based Voting System before the Runoff, in response to the request of electors pursuant to O.C.G.A. § 21-2-379.2(a), or initiating the reexamination process *sua sponte* before the Runoff, pursuant to O.C.G.A. § 21-2-379.2(a)..

191.

Abuse of discretion is found when a public official acts in an “arbitrary, capricious, and unreasonable” manner. Burke Cty. v. Askin, 291 Ga. 697, 701 (2012) (citing Massey v. Georgia Bd. of Pardons & Paroles, 275 Ga. 127, 128(2) (2002)). This includes acting in such an arbitrary, capricious way that their abuse of discretion “amounts to a failure on the part of the officer to exercise his discretion at all.” S. View Cemetery Ass'n v. Hailey, 199 Ga. 478, 483 (1945).

192.

Here, well before the Runoff, Kemp was informed of two breaches into CES system, that Russian agents were attempting to hack to U.S. elections, and overall that Georgia’s DRE Based Voting System was highly susceptible to attack based on the allegations stated throughout this Complaint. At the same time, Kemp admitted earlier this month that “anything is possible”²⁸ when it comes to Russians tapping into Georgia’s voting system.

193.

Despite this, Kemp declined help from the Department of Homeland Security to help protect Georgia’s DRE-based voting system in August 2016 (one of only two states to do so). He did because he does not “necessarily believe” and-- to this day--remains unconvinced that hacking of Georgia’s elections is a real

²⁸ Kim Zetter, Will the Georgia Special Election Get Hacked, Politico, June 14, 2017, <http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255> , (last visited June 30, 2017)

threat. About the issue he stated, “I think it was a politically calculated move by the [Obama] administration.”²⁹ His rationale for his belief? “The question remains whether the federal government will subvert the Constitution to achieve the goal of federalizing elections under the guise of security. [...] Designating voting systems or any other election system as critical infrastructure would be a vast federal overreach, the cost of which would not equally improve the security of elections in the United States.”³⁰

194.

Such beliefs are arbitrary in that they are based on a solely personal belief, capricious in that they could change on a whim, and unreasonable in that they are not rooted in fact and contrary to concerns expressed to him by his constituents, securities experts, and the Department of Homeland Security. They are so arbitrary, capricious, and unreasonable that they “amounts to a failure on the part of the officer to exercise his discretion at all.”

²⁹ Paul Waldman, How Democratic Timidity May Have Helped Trump Get Elected, Washington Post, June 23, 2017, https://www.washingtonpost.com/blogs/plum-line/wp/2017/06/23/how-democratic-timidity-may-have-helped-trump-get-elected/?utm_term=.d36b828f5d08 (last visited July 3, 2017)

³⁰ Allya Sternstein, At Least One State Declines Offer For DHS Voting Security, NextGov, August 25, 2016, <http://www.nextgov.com/cybersecurity/2016/08/some-swing-states-decline-dhs-voting-security-offer/131037/> (last visited July 3, 2017)

195.

Georgia's DRE-Based Voting System in question here was used in the 2016 General Election, the Special Election, and the Runoff. Upon information and belief, Kemp plans to use the system again in remaining 2017 elections, and beyond—despite being more than aware of the risk the system imposes on his constituents' right to vote.

196.

The Secretary of State is clearly charged with ensuring the safety and accuracy of our elections, but willfully denies known threats to Georgia's election process (against the wise counsel of the Federal Government, security experts, and his constituents). His misinformation and false assurances delivered to the General Assembly likely caused elected representatives to rely on Kemp's representations. Kemp's beliefs and political posturing has caused him to do essentially nothing to ensure the safety and accuracy of Georgia's voting systems. Such inaction is an abuse of discretion. See S. View Cemetery Ass'n v. Hailey, 199 Ga. 478, 483 (1945).

197.

Where the question is one of public right and the object is to procure the enforcement of a public duty, no legal or special interest need be shown, but it

shall be sufficient that a plaintiff is interested in having the laws executed and the duty in question enforced. O.C.G.A. § 9-6-24.

198.

The Court has full and complete power to issue mandamus under O.C.G.A. § 9-6-20, which provides, “All official duties should be faithfully performed; and whenever, from any cause, a defect of legal justice would ensue from a failure to perform or from improper performance, the writ of mandamus may issue to compel a due performance, if there is no other specific legal remedy for the legal rights.”

199.

Apart from this Court’s issuance of the writ of mandamus, Plaintiffs have no other legal remedy to compel enforcement of Defendant Kemp’s official, public duty to conduct the reexamination required by O.G.C.A § 21-2-379.2(b). They have attempted multiple times to have Defendant Kemp reevaluate the system, but he has resisted their request, and claimed impractical fees and timelines when he did respond, as a reason not to reevaluate. Additionally, Defendant Kemp can act on his own accord. Electors cannot force him to act in that capacity. Only the Court can.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs ask this court:

- to grant declaratory relief deeming that Defendants have violated the Georgia Constitution, 42 U.S.C. § 1983, Georgia's election code, including its recanvassing and certification regulations and provisions;
- to grant injunctive relief requiring that certification of results of the recent Congressional District 6 elections and the election itself be declared void *ab initio*, and enjoining the future use of Georgia's DRE-Based Voting System; and
- to issue a writ of mandamus for Defendant Kemp to fulfill his public duty to reexamine this system and its fundamental irregularities; and to grant all other relief this court deems proper.

Respectfully submitted this 3rd day of July 2017.

/s/ Bryan M. Ward
Bryan Ward, Esq.
Georgia Bar No. 736656
Marvin Lim, Esq.
Georgia Bar No. 147236
Holcomb + Ward LLP
3399 Peachtree Rd NE, Suite 400
Atlanta, GA 30326
(404) 601-2803 (office)

(404) 393-1554 (fax)
Bryan.Ward@holcombward.com
Marvin@holcombward.com

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)
Plaintiffs,)
v.) CIVIL ACTION
BRIAN P. KEMP, in his individual capacity) FILE NO.:
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
Defendants.)

VERIFICATION

I, DONNA CURLING, plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 30 day of June 2017

Donna Curling
DONNA CURLING

Sworn to and subscribed before me
this 30th day of May 2017.

[Signature]
Notary Public



STATE OF GEORGIA

Case 1:17-cv-02989-AT Document 1-2 Filed 08/08/17 Page 84 of 158

DONNA CURLING, an individual, et al.)
Plaintiffs,)
v.) CIVIL ACTION
BRIAN P. KEMP, in his individual capacity) FILE NO.:
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
Defendants.)

VERIFICATION

I, MARILYN MARKS, executive director and an officer of COALITION FOR GOOD GOVERNANCE, a plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 30 day of June 2017



MARILYN MARKS

Sworn to and subscribed before me
This 30th day of June 2017.

Willa F. Sullivan
Notary Public

Willa F. Sullivan
Notary Public
Mecklenburg County, NC

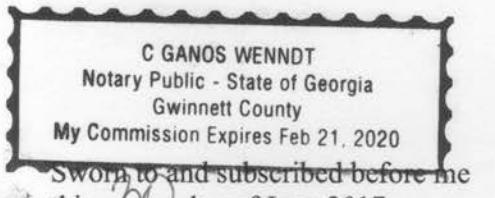
IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)	CIVIL ACTION FILE NO.:
)	
Plaintiffs,)	
)	
v.)	
)	
BRIAN P. KEMP, in his individual capacity)	
and his official capacity as Secretary of)	
State of Georgia and Chair of the)	
STATE ELECTION BOARD, et al.,)	
)	
Defendants.)	

VERIFICATION

I, DONNA PRICE, plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 30 day of June 2017



Sworn to and subscribed before me
this 30 day of June 2017.



Notary Public

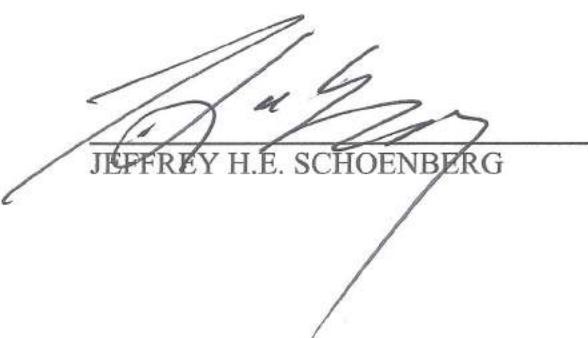
IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)
)
Plaintiffs,)
)
v.) CIVIL ACTION
)
BRIAN P. KEMP, in his individual capacity) FILE NO.:
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
)
Defendants.)

VERIFICATION

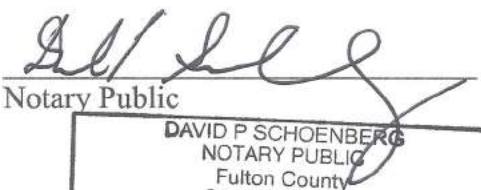
I, JEFFREY H.E. SCHOENBERG, plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 30th day of June 2017

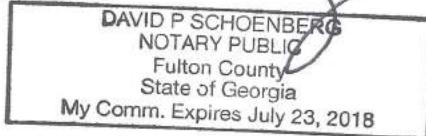


JEFFREY H.E. SCHOENBERG

Sworn to and subscribed before me
this 30th day of June 2017.



Notary Public



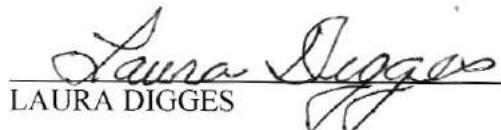
IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)
)
Plaintiffs,)
)
v.) CIVIL ACTION
) FILE NO.:
BRIAN P. KEMP, in his individual capacity)
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
)
Defendants.)

VERIFICATION

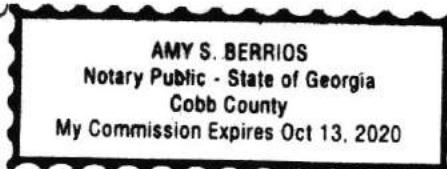
I, LAURA DIGGES, plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 30 day of June 2017


LAURA DIGGES

Sworn to and subscribed before me
this 30 day of June 2017.


Notary Public



Notarization validates
signature only,
not document content.

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)
)
Plaintiffs,)
)
v.)
)
BRIAN P. KEMP, in his individual capacity) CIVIL ACTION
and his official capacity as Secretary of) FILE NO.:
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
)
Defendants.)

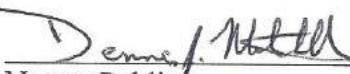
VERIFICATION

I, WILLIAM DIGGES III, plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

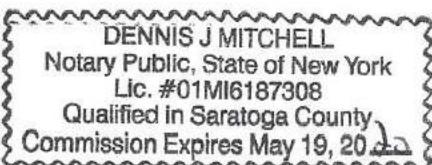
Dated this 30th day of June 2017


WILLIAM DIGGES III

Sworn to and subscribed before me
this 30th day of June 2017.



Notary Public



IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.)
)
Plaintiffs,)
)
v.) CIVIL ACTION
)
) FILE NO.:
BRIAN P. KEMP, in his individual capacity)
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
)
Defendants.)

VERIFICATION

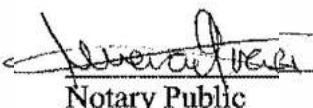
I, RICARDO DAVIS, plaintiff in the above-styled case, personally appeared before the undersigned notary public, duly authorized to administer oaths, and state under oath that every fact alleged in the **VERIFIED COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND WRIT OF MANDAMUS**, attached hereto, is true and correct to the best of my knowledge, information, and belief, except for any fact that also states a legal conclusion.

Dated this 30 day of June 2017



RICARDO DAVIS

Sworn to and subscribed before me
this 30 day of June 2017.



Notary Public



EXHIBIT A

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)
)
Plaintiffs,)
)
v.) CIVIL ACTION
) FILE NO.:
BRIAN P. KEMP, in his individual capacity)
and his official capacity as Secretary of)
State of Georgia and Chair of the)
STATE ELECTION BOARD, et al.,)
)
Defendants.)

AFFIDAVIT OF LOGAN LAMB

County of Fulton)
) ss.
State of Georgia)

LOGAN LAMB ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am a cybersecurity researcher based in Atlanta. I have a BS and MS in computer engineering from University of Tennessee, Knoxville. I have worked professionally in cybersecurity since 2010. I started at Oak Ridge National Lab in the Cyber and Information Security Research group. At CISR I specialized in static and symbolic analysis of binaries. I also worked with embedded systems security and conducting security assessments for the federal government. I left ORNL in 2014 and joined Bastille Networks, a local startup where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

2. On August 23, 2016 I went to 130 Peachtree Street in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conduct a wireless security

assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment is managed by the Center for Election Systems at KSU.

3. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the Center for Election Systems public website to see if there were any public documents that could give me background on CES and Merle King. I used the search “site:elections.kennesaw.edu inurl:pdf” at www.google.com and discovered what appeared to be files relating to voter registration cached by google.

4. After this discovery, I wrote a quick script to download what public files were available here: <https://elections.kennesaw.edu/sites/>, at the time a publicly accessible site. After running the script to completion I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:
 - voter registration databases filled with personally identifiable information of voters (filename *PollData.db3*)
 - Election Management System GEMs databases (.gbf and .mdb extensions)
 - PDFs of election day supervisor passwords, for example:
 - *July 2016 Primary and NP Election Runoff Password Memo.pdf*
 - Windows executables and DLLs, for example:
 - *System.Data.SQLite.DLL*
 - *ExpDbCreate.exe*
 - *ExpReport.exe*

5. Besides leaking information, the server at elections.kennesaw.edu was running a version of Drupal vulnerable to an exploit called drupageddon. Using drupageddon, an attacker can fully compromise a vulnerable server with ease. A

public advisory for drupageddon was release in 2014, alerting users that attackers would be able to execute, create, modify, and delete anything on the server.

On August 28, 2016 I sent an email to Merle King notifying him of the vulnerabilities I found.

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: <https://www.bastille.net/>. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"

I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install. Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"

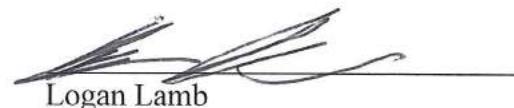
The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
<https://www.drupal.org/project/drupalgeddon>
<https://www.drupal.org/SACORE-2014-005>

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

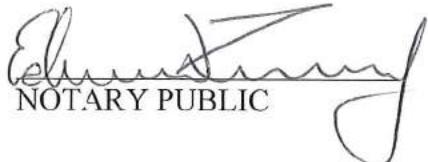
6. After having a brief conversation with Mr. King on August 29, 2016 and being assured that the issues would be remediated, I dropped the issue.

7. In late February, 2017 I told my colleague Chris Grayson about what transpired in August. He quickly confirmed the leaking of information had not been appropriately remediated. I tweaked my script and checked to see if it worked as it had in August.
8. The script was able to download the publicly available information. The data downloaded included the same data from the previous collection and new information relating to recent elections including:
 - More recent GEMs database files
 - Files relating to the presidential election, e.g.
 - *November 2016 General Election Day Password Memo.pdf*
 - *November 2016 General Voter Lookup Password Memo.pdf*
 - Very recent files, e.g. *064 (1-10-2017).pdf*
9. Given the severity and ease with which an attacker can use drupageddon, an attacker would have easily been able to gain full control of the server at elections.kennesaw.edu had they so wanted.
10. Having gained control of the server, an attacker could modify files that are downloaded by the end users of the website, potentially spreading malware to everyone who downloaded files from the website.
11. In addition to the previously mentioned files on the server, there were multiple training videos. One of these training videos instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.
12. Further Affiant sayeth not.



Logan Lamb

Sworn before me this 30 day of June, 2017, in June.



Edward Tinsley
NOTARY PUBLIC



EXHIBIT B

Subject: Re: Traffic footprints

Got it, thanks!

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
agreen57@kennesaw.edu
<http://coles.kennesaw.edu/faculty/green-andrew.php>

Mr. Andrew Green | Coles College of Business | Kennesaw ...

coles.kennesaw.edu

Publications. Hands-on Information Security Lab Manual, Fourth Edition; Addressing Emerging Information Security Personnel Needs. A Look at Competitions in ...

Ph: 470-578-4352
Burruss Building, Room #490

From: "Chris Grayson" <cegrayson3@gmail.com>
To: "agreen57" <agreen57@kennesaw.edu>
Sent: Thursday, March 2, 2017 7:58:49 PM
Subject: Traffic footprints

Hey Andy,

As discussed, here are the times at which we generated traffic to the web server:

Wednesday 02/22/17 - 6:00PM - 12:00AM EST - traffic originated from an Atlanta IP address and an IP address from Switzerland
Friday 02/24/17 - 12:00PM - 8:00PM EST - traffic originated from an Atlanta IP address
Tuesday 02/28/17 - 5:00PM - 12:00AM EST - traffic originated from an Atlanta IP address
Wednesday 03/01/17 - 7:00PM - 10:00PM EST - traffic originated from an Atlanta IP address

All of this traffic was either (1) browsing open directories or (2) retrieving files from those directories.

Best regards,

Christopher Grayson
Founder, Web Sight.IO
Software and Security Engineer
(678) 462 - 9770

EXHIBIT C



Center for Election Systems

Incident Date: March 1, 2017

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

KENNESAW, Ga (Mar. 31, 2017)—Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."



UI TS Information Security Office
Financial Impact

Center for Election Systems

Incident Date: March 1, 2017

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately \$2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UI TS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UI TS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)

Action Item Owner(s): UI TS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UI TS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UI TS ISS Staff Members.

Action Item Owner: UI TS-ISO, UI TS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard



UITS Information Security Office

Center for Election Systems

Incident Date: March 1, 2017

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.

Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. Issue: Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.

Action Item Owner: UITS-ISO, CES Staff

5. Issue: Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.

Action Item Owner: UITS-ISO, KSU UPD, CES Staff

6. Issue: The elections private network data closet contains a live network jack to the [REDACTED] (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.

Action Item Owner: UITS-ISO, UITS-ISS

7. Issue: A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.

1. Rackmount UPS Battery backups (one displaying warning light)

Recommendation: Replace batteries as needed and move under UITS ISS management

2. 3com Switches – Age 10+ years -- No Support -- L2 only

Recommendation: Replace and move under UITS ISS management

3. Dell 1950 (Windows Domain Controller) – Age 10+ years

Recommendation: Surplus

4. Dell PowerEdge R630 – Age 1 year

Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network

5. EPIC – Vision Computer – Age Unknown – Ballot creation box

Recommendation: Continue as ISO/CES managed

6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups

Recommendation: Surplus

7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS

Recommendation: Surplus

8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610



UI TS Information Security Office

Center for Election Systems

Incident Date: March 1, 2017

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950

Recommendation: Surplus

10. Web server backup

Recommendation: Surplus

Action Item Owner: UI TS-ISO, UI TS-ISS, CES Staff

8. Issue: An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UI TS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

Action Item Owner: UI TS-ISO, UI TS-ISS, CES Staff

9. Issue: A wireless access point was found when UI TS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UI TS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

Action Item Owner: UI TS-ISO, UI TS-ISS

10. Issue: Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone

Green = KSU data public network

Blue = Elections private network

White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately \$3,000.

Action Item Owner: UI TS-ISO, UI TS-ISS

EXHIBIT D



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

C. Ryan Germany
GENERAL COUNSEL

June 5, 2017

VIA U.S. MAIL

Mustaque Ahamad
898 Kings Ct NE
Atlanta, GA 30306

David Bader
1824 Charline Ave NE
Atlanta, GA 30306

Ricardo Davis
206 Hunters Mill Lane
Woodstock, GA 30188

Richard DeMillo
2500 Peachtree Rd NW
Unit 606
Atlanta, GA 30305

Virginia Forney
59 Park Lane NE
Atlanta, GA 30309

Merrick Furst
1707 Wildwood Rd NE
Atlanta, GA 30306

Adam Ghetti
606 E. Morningside Drive
Atlanta, GA 30324

Jeff Levy
916 Kings Ct., Unit 1201
Atlanta, GA 30306

Rhonda J. Martin
2500 Peachtree Rd NW
Suite 606
Atlanta, GA 30305

Paul Nally
3667 Hwy 140
Rydal, GA 30171

Michael Opitz
1802 Wynfair Ct.
Marietta, GA 30062

Re: Request for Reexamination of Voting System

Dear Electors,

As the electors who requested a reexamination of the direct recording electronic voting system used throughout Georgia, I wanted to update you on how the Secretary of State's office intends to comply with that request in accordance with O.C.G.A. § 21-2-379.2. Such a request has never been made until now, so I appreciate you bearing with us as we determine the best way to undertake a robust and cost-effective reexamination of the system that includes 27,000 voting machines across the state of Georgia.

Your request differs from requests to review direct recording electronic voting systems prior to being used in Georgia, as the system that you seek to have reexamined has already been deployed statewide. Therefore, a reexamination of that system should be broad enough so that a significant confidence level may be had in the final report. We estimate that such a review will

Letter to Electors

June 5, 2017

Page 2 of 2

cost \$10,000 and will take six months to complete. This estimate is subject to revision as we conduct the reexamination.

You also requested a copy of the most recent certification documentation for the current voting system. Copies of those documents are available for you to review at your convenience at the Office of the Secretary of State, Elections Division, 2 MLK Jr. Dr., Suite 802, West Tower, Atlanta, Georgia, 30334.

Thank you for your interest in Georgia's elections.

Sincerely,

A handwritten signature in blue ink, appearing to read "C. RYAN GERMANY".

C. Ryan Germany

Cc: Marilyn Marks (marilyn@aspenoffice.com) via email
Dr. Duncan Buell (buell@acm.org) via email

EXHIBIT E

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)	
)	
Plaintiffs,)	
)	
v.)	CIVIL ACTION
)	FILE NO.:
BRIAN P. KEMP, in his individual capacity)	
and his official capacity as Secretary of)	
State of Georgia and Chair of the)	
STATE ELECTION BOARD, et al.,)	
)	
Defendants.)	

AFFIDAVIT OF EDWARD W. FELTEN

EDWARD W. FELTEN ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the Director of Princeton's Center for Information Technology Policy. I received my Ph.D. in Computer Science and Engineering from the University of Washington in 1993. I am a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

2. From 2015 until January 2017, I served in the White House as Deputy United States Chief Technology Officer. During that time I advised the President and his senior advisors on policy issues relating to computer science, including issues relating to the security and reliability of elections and electronic voting systems.

3. A copy of my curriculum vitae is attached as Exhibit A.

Inherent risks of paperless electronic voting machines

4. Before turning to the systems and circumstances specific to Georgia elections, I will provide a brief summary of cybersecurity issues relating to voting machines.

5. The voting machines at issue are a type of so-called Direct Recording Electronic (DRE) machine. DREs are voting machines that are designed to record a voter's ballot directly in electronic storage, without creating any record of the ballot that can be directly verified by the voter.

6. DREs can be contrasted with other voting technologies in which there is a record of the voter's ballot, typically on paper, the accuracy of which can be verified directly by the voter in the polling place, and which is collected at the polling place as a record of the voter's intent. The most common examples of voter-verifiable ballots include paper ballots. Paper ballots can be tabulated by hand counting. Alternatively, they can be tabulated securely by a machine such as an optical scanner, provided that a post-election audit is performed to confirm that the machine count is consistent with the results of manually inspecting a suitable sample of paper ballots.

7. The lack of a voter-verifiable ballot creates special risks associated with any DRE voting system. For this reason, computer scientists and cybersecurity experts typically recommend against the use of DREs. I concur with this general recommendation against the use of DREs.

8. The hardware of a DRE—the physical equipment comprising the computer—is much like a standard desktop computer, often installed into a different physical enclosure. Like a standard computer, a DRE will do whatever the software installed in it directs it to do. If anyone changes the software, whether through malice or error, the DRE may do something other than accurately recording and tabulating votes.

9. A malicious modification to a DRE's software would likely cause the DRE to modify ballots silently. The modified software could be designed to report on the machine's display screen, to voters and election officials, that all was well. It could also be designed to falsify all of the logs and records kept by the voting machine.

10. My students and I have modified the software on many types of DREs. For example, my students modified a (now decommissioned) New York DRE to turn it into a kiosk for playing the popular arcade game Pac-Man. We have also created, installed, and tested software for multiple DRE models that would silently modify election results. (For obvious reasons, these latter tests were done in secure laboratories.)

My team's study of Diebold voting machines

11. I led a team of researchers that studied the Diebold AccuVote TS voting machine system. We published a peer-reviewed paper summarizing our analysis, which is attached as Exhibit B.

12. As part of our research we demonstrated that it was possible to create a voting machine virus: a computer virus that infected the voting machines, spreading from machine to machine by infecting the memory cards that are used to transport election and ballot information between the machines and central tabulation offices. The virus, having infected a voting machine, would modify election results, without leaving any trace in the logs or records kept by the machine. We created and tested such a virus in our secure laboratory.

13. The voting machine virus we created could spread from machine to machine even though the machines were never connected to any network. The virus would spread by infecting memory cards that were transported between machines. When a memory card was inserted into an infected machine, the virus would infect the memory card. When an infected memory card was inserted into a previously unaffected machine, the virus would infect this machine. Thus the memory cards acted as carriers for the virus, much as mosquitoes act as carriers for some human diseases.

14. The notion that machines not connected to the Internet are somehow immune to viruses or other security compromise is a fallacy. It is inconsistent with decades of experience with cybersecurity. In the specific case of Georgia voting machines, it is directly disproven by the research in my laboratory.

15. I did a live demonstration of this election-stealing virus, including showing the casting of votes and mis-reporting of the vote counts by the machine, during live testimony at a hearing of a committee of the U.S. House of Representatives. My students and I did a similar demonstration twice on live television, on CNN and Fox News.

16. The TS machine we studied allowed modified (and possibly malicious) software to be installed by anyone who could open a small metal access door on the side of the machine. The door was locked by an ordinary file cabinet type of lock. Because the very same key that is used for the access door on the AccuVote TS is also used widely on office furniture, jukeboxes, and hotel minibars, the keys are easily purchased. I bought a gross of these keys (i.e., 144 keys) from a vendor on the Internet. The lock is also easily picked—a member of our team who studies locks as hobby was able to pick the access door lock consistently in less than 15 seconds.

17. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes.

18. Our peer reviewed paper listed a number of other security problems with the AccuVote TS system. Some of these problems could in principle be fixable by improving the software of the TS, but others are inherent in the machine's hardware and therefore not fixable by any software update.

19. As described in our peer reviewed paper, it is inherent in the hardware design of the TS that a person who can get physical access to the inside of the machine can install any software they like on the machine.

20. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes. This problem is inherent in the hardware design of the TS machine.

21. Subsequent to the publication of our paper, we studied the AccuVote TSX system and found that it had similar security problems.

Need for software verification

22. One cannot know that any DRE machine, including a TS or TSX, will accurately record or tabulate votes, unless one is certain as to which software is installed on that machine. Because of the ease of malicious modification of the software, it is not enough to know which software is supposed to be installed—one must inspect the machine to verify which software is actually installed.

23. Verifying which software is actually installed is technically very difficult, because one cannot rely on the software itself to report its own status accurately. Malicious software can simply misreport its own status, reporting that everything is normal. Relying on the software to report whether it has been tampered with is like trying to determine whether a person is honest by asking him, “Are you honest?” An answer of “yes” is not reliable evidence.

24. Unfortunately, the standard methods for inspecting the software version installed in a machine rely on the machine’s software in one way or another, so they fail to avoid this pitfall and should not be trusted. Special protocols, typically involving the use of specialized equipment, must be designed and used to perform such inspections, and rigorous chain-of-custody controls are necessary after the inspection to make sure no tampering with the machine’s software could have occurred after the inspection.

25. Unless all of these steps are followed, with respect to a particular DRE machine, one cannot be confident in its ability to accurately record or tabulate votes.

Need for secure facilities

26. I understand that Georgia voting machines are tested and configured in the Center for Election Systems (CES) at Kennesaw State University (KSU). Because my team’s research has demonstrated the propagation of malicious software during these types of activities, including propagation to systems not directly connected to the Internet, any security breach at CES, or failure to implement adequate cybersecurity precautions at CES, could have created an opportunity for a malicious party to modify software in voting machines and related systems.

27. The security breach at CES, and KSU’s response to it, are indications that cybersecurity precautions at CES may not have been adequate. It is significant that KSU’s response to the breach included steps to change how cybersecurity and system administration were managed at CES, so that CES personnel were no longer managing these functions on their own. It is significant that the post-breach report from KSU’s Information Security Office listed as its first “Opportunit[y] for Improvement” the “Poor understanding of risk posed by [CES] IT systems.”

28. The most sophisticated cyberattackers are especially skilled not only at gaining unauthorized access to systems, but also at maintaining access. So-called Advanced Persistent Threat actors specialize in gaining access and maintaining that access over time, while avoiding detection and waiting for the best moment to strike. Once they are in a system, it can be extraordinarily difficult to find them. As a result, very stringent measures may be necessary to

render a facility safe after a period of vulnerability—and especially when highly skilled actors may have been motivated to compromise that facility.

29. Because of the vulnerability of the DRE voting machines to software manipulation, and because of intelligence reports about highly skilled cyber-actors having attempted to affect elections in the United States, such precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism.

30. Further Affiant sayeth not.



Edward W. Felten

State of New Jersey
County of Mercer

Taylor J Cerverizzo, Notary Public



EXHIBIT F



OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do
hereby certify that*

the attached nine pages, labeled A through I, are true and correct copies
of voting equipment certifications; all as same appear on file in this office.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed
the seal of my office, at the Capitol, in the City of Atlanta,
this 18th day of April, in the year of our Lord Two
Thousand and Eight and of the Independence of the United
States of America the Two Hundred and Thirty-Second.



Karen C. Handel, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do
hereby certify that*

the attached one (1) page constitutes a true and correct copy of the certification of the AccuVote TS R6 Voting System, consisting of GEMS Version 1.1822G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, for use by the electors of the State of Georgia in all primaries and elections as provided in Georgia Election Code 21-2; all as same appear on file in this office.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 27th day of November, in the year of our Lord Two Thousand and Seven and of the Independence of the United States of America the Two Hundred and Thirty-Second.



A handwritten signature in black ink that reads "Karen C Handel".

Karen C. Handel, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10th day of July, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.



Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

For the purposes of a Conditional Interim Certification the AccuVote TS R6 and the AccuVote TSX Voting System, consisting of GEMS version 1.18.24, AVTS firmware version 4.6.4, and AVTS voting stations with the attached AccuView Printer Module (The following components of the Georgia voting system were included in the test to verify compatibility: GEMS 1.18.22G, AccuVote TS R6 voting stations with firmware AVTS 4.5.2, AccuVote TSX voting stations with AccuVote firmware AVTS 4.5.2, and ExpressPoll 4000 1.2.0.), manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; the Conditional Interim Certification shall expire on December 31, 2006.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 9th day of August, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.



Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 14th day of April, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirtieth.



Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.



Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.



A handwritten signature of Cathy Cox.

Cathy Cox, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby
certify that*

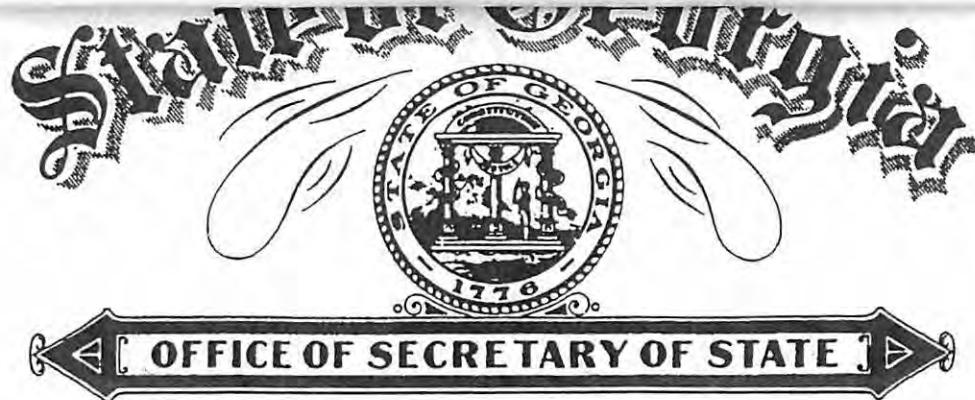
the AccuVote TS R6 Voting System, consisting of GEMS Version 1.18.22G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 31st day of December, in the year of our Lord Two Thousand and Four and of the Independence of the United States of America the Two Hundred and Twenty-Ninth.



A handwritten signature of Cathy Cox in black ink.

Cathy Cox, Secretary of State



[OFFICE OF SECRETARY OF STATE]

I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that

the AccuVote TS R6 Voting

System, consisting of GEMS Version 1.18.15, and the AVTS firmware, Version 4.3.14, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed
the seal of my office, at the Capitol, in the City of Atlanta, this
10th day of February , in the year of our Lord
Two Thousand and Three
and of the Independence of the United States of America the
Two Hundred and Twenty-ninth



A handwritten signature of Cathy Cox.

SECRETARY OF STATE



[OFFICE OF SECRETARY OF STATE]

I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that

the AccuVote TS R6 Voting

System, consisting of the AVTS firmware, Version 4.1.11, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

~~~~~

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed  
the seal of my office, at the Capitol, in the City of Atlanta, this  
23<sup>th</sup> day of May , in the year of our Lord  
Two Thousand and Two  
and of the Independence of the United States of America the  
Two Hundred and Twenty-sixth



*Cathy Cox*

SECRETARY OF STATE

## EXHIBIT G

**AFFIDAVIT OF DUNCAN A. BUELL**

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of the petition to void the June 20, 2017, election and to prohibit further use of Georgia's current DRE voting system..

2. In my opinion, the Diebold electronic voting system used in Georgia is vulnerable both to malicious interference and inadvertent error. The Diebold system in general has been put under technical scrutiny several times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has been successful.

3. The possible stamp of approval (for a modified system?) given by the Kennesaw State University (KSU) Center for Election Systems (CES) does not in my opinion mitigate for use in Georgia the known flaws of the system. Indeed, the recent reports from the Kim Zetter article for *Politico* seem to demonstrate that the KSU CES has been either unable or unwilling to address security, privacy, and integrity issues even when they have been privately disclosed to the CES by credible cybersecurity professionals. The fact that the FOIA request of Mr. Garland Favorito yielded only three emails between CES and Mr. Logan Lamb and Mr. Christopher Grayson suggests further that CES might not have been taking seriously the security threats that were pointed out by Lamb and Grayson.

### **Qualifications and Relevant Employment History**

4. In 1971, I earned a B.S. in Mathematics from the University of Arizona.

The following year, I earned an M.A. in Mathematics from the University of Michigan.

In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at <http://www.cse.sc.edu/duncanbuell>.

5. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

6. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics

different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then “the largest single computation ever made” in the U.S. intelligence community.

7. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

8. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

9. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued. When

the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well. I have obtained and analyzed the data from the 2012, 2014, and 2016 elections in South Carolina, and I have also analyzed ES&S DRE-voting system data in more limited quantities from Colorado, North Carolina, Pennsylvania, and Texas.

### **Basis for My Opinions**

10. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

11. I have also used for my opinions a review of the documents surrounding the KSU CES hack in Spring 2017, including the report attached to an email on 24 April 2017 from Stephen Gay to Merle King.

### **The Diebold Election System Was Unacceptable for Use in the CD6 Election Held 20 June 2017**

12. I begin with the fact that the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems. The letter from Georgia citizens to Secretary of State (SoS) Brian Kemp on 10 May 2017 cites the security analysis of

Felcman, Halderman, and Felten. The GEMS central server software analysis by Ryan and Hoke, cited in the same letter, shows flaws in the central server. The fact that all analyses of the “standard” Diebold election system, even operated in intended conditions, have found major flaws should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.

13. Evidence indicates that the April 18 and June 20 Special Elections were conducted using a “non-standard” customized Diebold DRE voting system, with an unusual configuration, not tested by a federally accredited laboratory.

14. Even more alarming is the fact that the CES server containing crucial election programming files was known to be open to entry and manipulation in August 2016, and this glaring security problem had not been corrected even as late as March 1, 2017.

15. We must assume that the failure to secure the system and its data caused the already unreliable and unfit system unquestionably to be vulnerable to undetected attack. The system must be considered compromised and it is only prudent that the system must be considered to have been compromised from August 2016 through March 2017, and should not be used to conduct a public election.

16. It has been well-established in the computer security world that the Diebold election system, as configured for “standard” use, is unfit for use due to security and reliability concerns. In my letter/request to Secretary Kemp, serving as a technical advisor to the citizens of Georgia who had petitioned for the non-use of the Diebold

systems in the 20 June 2017 election, I asked for responses to the questions of security and reliability. If the standard system had been modified by CES, and that system had been re-certified, and one could rely upon the security credentials of the KSU CES, then one might have some limited confidence in the suitability of the Diebold system for use in elections in Georgia.

17. The response from Secretary Kemp has been tepid at best. His letter of June 5, 2017, does not address technical questions, and does not really address the questions posed by the electors of Georgia in their original request to him.

18. To be specific, the report of 18 April 2017, attached to Mr. Gay's email to Merle King, is damning in what it says and what it does not say. What we see as "successes" are only that the response to a security incident went well. This is essentially the statement that when law enforcement officials arrived at the barn, they found the door closed, and they found no horses inside the barn, but they had arrived quickly.

19. We see a number of issues in the 18 April 2017 report that indicate that the KSU CES security protocols were insufficient, and we find no commentary on any of those protocols that might have mitigated the damage.

20. I do not see that there are technical comments about successful, or positive, security measures that would have mitigated the potential damage done by the fact that the CES system was apparently open to attack for an extended period by any determined actor.

21. Indeed, the report can be read to suggest that the CES was not following some of the most basic security practices taught to all undergraduates in a computer

security course. Issues 1 and 8, under "Opportunities for Improvement", for example, cite a poor understanding of risk and of asset value on a main server and a failure to perform a security assessment. This apparent failure to know and to understand basic principles of security would not be inconsistent with Mr. Lamb's account that sensitive data was still openly available months after he had notified CES of this major security problem.

22. We come to the bottom line. We know, because it has been shown repeatedly, that the Diebold system as it is standardly configured, has major flaws. We would believe, based on our knowledge of process in Georgia, that it is the responsibility of the KSU CES to mitigate (or perhaps even remove?) these major flaws. But we do not see, in the report regarding the operational practices of the CES, that there is reason to believe that they have in fact mitigated the known flaws, produced a system that has been federally or state certified, and provided to the citizens of Georgia an election system in which they can be confident. For these reasons, the voting system in use cannot reasonably be approved as "safe and accurate for use" as required by Georgia statute.

23. For these reasons, I would argue that the Diebold system ought not be used in elections unless and until a complete security analysis has been performed on the software and hardware and a complete verification and integrity check has been made of the databases, including voter registration databases. Nor should the reported results generated by the system be relied on for a determination of the outcome of the June 20 special election.

24. I affirm that the foregoing is true and correct.

A handwritten signature in blue ink, appearing to read "Jimmie Powell", is written over a horizontal line.

DUNCAN BUELL

Date

Sworn before me this 29th day of June, 2017, in Columbia, SC.

Rebecca Mayo  
NOTARY PUBLIC

## EXHIBIT H

May 24, 2017

The Honorable Brian Kemp  
214 State Capitol  
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 14<sup>th</sup> we sent a letter to you expressing grave concerns regarding the security of Georgia's voting systems and requesting transparency from your office concerning key questions about the reported breach at Kennesaw State University Center for Election Systems (KSU).

The FBI has reportedly closed its investigation into the breach at KSU and will not be pressing federal charges<sup>1</sup> but regrettably little more is known. We remain profoundly concerned about the security of Georgia's votes and the continued reliance on Diebold paperless touchscreen voting machines for upcoming elections.<sup>2</sup>

The FBI's decision not to press charges should not be mistaken for a confirmation that the voting systems are secure. The FBI's responsibility is to investigate and determine if evidence exists indicating that federal laws were broken. Just because the FBI concluded this hacker did not cross that line does not mean that any number of other, more sophisticated attackers could not or did not exploit the same vulnerability to plant malicious software that could be activated on command. Moreover, the FBI's statement should not be misinterpreted to conclude that KSU or the Georgia voting system do not have other security vulnerabilities that could be exploited by malicious actors to manipulate votes.

Any breach at KSU's Election Center must be treated as a national security issue with all seriousness and intensity. We urge you to engage the Department of Homeland Security and the US Computer Emergency Readiness Team (CERT) to conduct a full forensic investigation. We cannot ignore the very real possibility that foreign actors may be targeting our election infrastructure.

The FBI investigation lasted a mere few weeks. It's our understanding that this investigation was designed to determine whether criminal charges should be brought. However, a truly comprehensive, thorough and meaningful forensic computer security investigation likely would not be completed in just a few weeks, and it could take many months to know the extent of all vulnerabilities at KSU, if any have been exploited and if those exploits extended to the voting systems. Time and again cyber breaches are found to have been far more extensive than initially reported. When the breach at the Office of Personnel and Management was discovered in March of 2014 it was not disclosed to the public because officials concluded (incorrectly) that there was no loss of personal identifying information. The system was then reviewed by a private security

---

<sup>1</sup> Torres, Kristina, "Feds: "Security Researcher" behind KSU data breach broke no federal law," *Atlanta Journal Constitution*, March 31, 2017

<sup>2</sup> Diamond, Aaron, "KSU takes back seat in Georgia elections after server hack," *WSB-TV2 Atlanta News*, March 17, 2017

firm which determined in May (again incorrectly) that the system's security was sound.<sup>3</sup> One month later news reports surface warning that 25,000 individuals' personnel records have been compromised. A year later, that number had grown to over 21 million plus the fingerprints of 5.6 million employees.<sup>4</sup>

Problems reported during the April 18<sup>th</sup> special election have only escalated our concerns. According to news reports, an error occurred during the uploading of votes in Fulton County on election night.<sup>5</sup> Fulton's director of registration and elections, claimed that when a memory card was uploaded to transfer vote totals the operation failed and the system generated an error message that was "gobbledygook, just junk, just letters."<sup>6</sup> This sort of error message could be the result of a corrupted database and more investigation is needed.

While one cause of database corruption could be cyber intrusion which should not be ruled out, it is important to note that it was documented over ten years ago that the Diebold GEMS database used in Georgia is vulnerable to database corruption, especially if databases are run concurrently<sup>7</sup> as reportedly occurred in the recent special election.<sup>8</sup> This is because GEMS was built on Microsoft JETS database software, an outdated database which cannot be relied upon to provide accurate data.

According to Microsoft:

*"When Microsoft JETS is used in a multi-user environment, multiple client processes are using file read, write, and locking operations on a shared database. Because multiple client processes are reading and writing to the same database and because JETS does not use a transaction log (as do the more advanced database systems, such as SQL Server), it is not possible to reliably prevent any and all database corruption."*[Emphasis added.]

The voting system database stores the vote data. Corruption of the database could mean vote data, or vote counts, are lost. Because Georgia still relies on touchscreen voting machines that do not provide a paper ballot, if votes data is corrupted, it is possible that vote totals could be lost and without a physical paper ballot, there is no way to restore and correct the vote count.

This would be an excellent time to move with all expediency to replace Georgia's outdated voting system, to adopt paper ballot voting and implement robust manual post-election audits. The threat that foreign hackers might target the Dutch national elections caused the Netherlands

<sup>3</sup> "Timeline: What We Know about the OPM Breach," *NextGov.com*, <http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/>

<sup>4</sup> Rosenfeld, Everett, "Office of Personnel and Management: 5.6 million estimated to have fingerprints stolen in breach," *CNBC*, September 23, 2015

<sup>5</sup> Kass, Arielle, "'Rare error' delays Fulton County vote count in 6<sup>th</sup> district race," *Atlanta Journal Constitution*, April 19, 2017

<sup>6</sup> *Ibid.*

<sup>7</sup> Hoke, Candice, Ryan, Thomas, "GEMS Tabulation Database Design Issues in Relation to Voting System Certification Standards," [https://www.usenix.org/legacy/event/evt07/tech/full\\_papers/ryan/ryan.pdf](https://www.usenix.org/legacy/event/evt07/tech/full_papers/ryan/ryan.pdf)

<sup>8</sup> Kass, Arielle, "'Rare error' delays Fulton County vote count in 6<sup>th</sup> district race," *Atlanta Journal Constitution*, April 19, 2017

<sup>9</sup> How to Troubleshoot and to Repair a Damaged Access 2002 or Later Database, (Rev. 6.1 2006) at <http://support.microsoft.com/default.aspx?scid=kb;en-us;283849>

to cancel all electronic voting and hold its March elections on paper ballots. The U.S. has not responded to the threat of foreign hacking with the same accountability and speed. The former director of U.S. national intelligence James Clapper recently told Congress that foreign hackers will continue to attack and we should expect them in the 2018 and 2020 elections.<sup>10</sup>

We believe this is a profoundly serious national security issue. We stand ready to help you any way we can to help protect our democratic process and regain the confidence of voters.

Sincerely,

Dr. Richard DeMillo  
Charlotte B, and Roger C. Warren Professor of Computing  
Georgia Tech

Dr. Andrew W. Appel  
Eugene Higgins Professor of Computer  
Science,  
Princeton University

Dr. David L. Dill  
Professor of Computer Science,  
Stanford University

Dr. J. Alex Halderman  
Professor, Computer Science and Engineering  
Director, Center for Computer Security and  
Society  
University of Michigan

Harri Hursti  
Chief Technology Officer and co-founder,  
Zytronite, and founding partner, Nordic  
Innovation Labs.

Dr. Douglas W. Jones  
Department of Computer Science  
University of Iowa

Dr. Duncan Buell  
Professor, Department of Computer Science  
& Engineering, NCR Chair of Computer  
Science & Engineering,  
University of South Carolina

Dr. Michael Fischer  
Professor of Computer Science,  
Yale University

Candice Hoke  
Co-Director, Center for Cybersecurity &  
Privacy Protection and Professor of Law,  
Cleveland State University

Dr. David Jefferson  
Lawrence Livermore National Laboratory

Dr. Joseph Kiniry  
Principal Investigator, Galois  
Principled CEO and Chief Scientist,  
Free & Fair

---

<sup>10</sup> Ng, Alfred, "Ex-intel chief James Clapper warns of more Russian hacks," *CNET*, May 8, 2017

Dr. Ronald L. Rivest  
MIT Institute Professor

Dr. Barbara Simons  
IBM Research (retired),  
former President Association for Computing  
Machinery (ACM)

Dr. Vanessa Teague  
Department of Computing & Information systems,  
University of Melbourne

Dr. John E. Savage  
An Wang Professor of Computer Science,  
Brown University

Dr. Philip Stark  
Associate Dean, Division of Mathematics and  
Physical Sciences,  
University of California, Berkeley

Affiliations are for identification purposes only, they do not imply institutional endorsements.

## EXHIBIT I

March 15, 2017

The Honorable Brian Kemp  
214 State Capitol  
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 3<sup>rd</sup> it was reported that the Federal Bureau of Investigations is conducting a criminal investigation into an alleged cyber attack of the Kennesaw State University Center for Election Systems. According to the KSU Center for Election Systems' website, "the Secretary of State authorized KSU to create a Center for Election Systems, dedicated to assisting with the deployment of the Direct Record Electronic (DRE) voting technology and providing ongoing support."<sup>1</sup> The Center is responsible for ensuring the integrity of the voting systems and developing and implementing security procedures for the election management software installed in all county election offices and voting systems.

The Center has access to most if not all voting systems and software used in Georgia. It also is responsible for programming these systems and accessing and validating the software on these systems. It is our understanding that the Center also programs and populates with voter records the electronic poll books used in polling places statewide. A security breach at the Center could have dire security consequences for the integrity of the technology and all elections carried out in Georgia.

In order for citizens to have faith and confidence in their elections, transparency is crucial, including about events such as the KSU breach, and its extent and severity. While we understand that this investigation is ongoing and that it will take time for the full picture to emerge, we request that you be as forthcoming and transparent as possible regarding critical information about the breach and the investigation, as such leadership not only will be respected in Georgia but also emulated in other states where such a breach could occur. We expect that you are already pursuing questions such as the following, regarding the breach, and trust that you will make public the results of such inquiry:

1. Can you estimate when the attacker breached KSU's system?
2. How did the attacker breach KSU's system?
3. How was the breach discovered?
4. Which files were accessed?
5. Were any files accessed that related to software or "hashes" for the voting machines?
6. Is there any evidence that files were modified? If so, which files?
7. Had KSU begun ballot builds for the upcoming special election?
8. To whom are these attacks being attributed? Could this be an insider attack? Has the FBI identified any suspects or persons of interest?

---

<sup>1</sup> <http://elections.kennesaw.edu/about/history.php>

9. Has the FBI examined removable media for the possibility of implanted malware?
10. Has the FBI examined the hash or verification program for tampering?
11. What mitigations are planned for the near- and long-term?

In any state an attack on a vendor providing software and system support with such far-reaching responsibilities would be devastating. This situation is especially fragile, because of the reliance on DRE voting machines that do not provide an independent paper record of verified voter intent. KSU has instead sought to verify the validity of the software on the voting machines by running a hash program on all machines before and after elections in an effort to confirm that the software has not been altered. However, if KSU's election programming were compromised, it is also possible that the verification program could have been modified to affirm that the software is correct, even if it were not. This is a risk of using software to check the correctness of software.

Of course all Georgia elections are important. This month and next include special elections as well. If these upcoming elections are to be run on DREs and e-pollbooks that are maintained and programmed by KSU while the KSU Center for Election Systems is itself the subject of an ongoing criminal investigation, it can raise deep concerns. And today's cyber risk climate is not likely to improve any time soon.

We urge you to provide Georgia's citizens with information they need to confirm before going to vote that their name will appear correctly on the voter rolls, as well as back-up printed voter lists in case anomalies appear. Most importantly, we urge you to act with all haste to move Georgia to a system of voter-verified paper ballots and to conduct post-election manual audits of election results going forward to provide integrity and transparency to all of Georgia's elections. We would be strongly supportive of such efforts and would be willing to help in any way we can.

Sincerely,

Dr. Richard DeMillo  
Charlotte B. and Roger C. Warren Professor of Computing  
Georgia Tech

Dr. Andrew W. Appel  
Eugene Higgins Professor of Computer  
Science,  
Princeton University

Dr. Duncan Buell  
Professor, Department of Computer Science  
& Engineering, NCR Chair of Computer  
Science & Engineering,  
University of South Carolina

Dr. Larry Diamond  
Senior Fellow, Hoover Institute and  
Freeman Spogli Institute, Stanford University

Dr. David L. Dill  
Professor of Computer Science,  
Stanford University

Dr. Michael Fischer

Dr. J. Alex Halderman

Professor of Computer Science,  
Yale University

Dr. Joseph Lorenzo Hall  
Chief Technologist,  
Center for Democracy & Technology

Harri Hursti  
Chief Technology Officer and co-founder,  
Zyptonite, and founding partner, Nordic  
Innovation Labs.

Dr. Douglas W. Jones  
Department of Computer Science  
University of Iowa

Dr. Justin Moore  
Software Engineer, Google

Dr. Ronald L. Rivest  
MIT Institute Professor

Bruce Schneier  
Fellow and lecturer  
Harvard Kennedy School of Government

Dr. Philip Stark  
Associate Dean, Division of Mathematics and  
Physical Sciences,  
University of California, Berkeley

Professor, Computer Science and Engineering  
Director, Center for Computer Security and  
Society  
University of Michigan

Candice Hoke  
Co-Director, Center for Cybersecurity &  
Privacy Protection and Professor of Law,  
Cleveland State University

Dr. David Jefferson  
Lawrence Livermore National Laboratory

Dr. Joseph Kiniry  
Principal Investigator, Galois  
Principled CEO and Chief Scientist,  
Free & Fair

Dr. Peter G. Neumann  
Senior Principal Scientist, SRI International  
Computer Science Lab, and moderator of the  
ACM Risks Forum

Dr. John E. Savage  
An Wang Professor of Computer Science,  
Brown University

Dr. Barbara Simons  
IBM Research (retired),  
former President Association for Computing  
Machinery (ACM)

Dr. Vanessa Teague  
Department of Computing & Information  
systems, University of Melbourne

Affiliations are for identification purposes only, they do not imply institutional endorsements.

## EXHIBIT J

**George Balbona**  
180 Mathews Circle, Marietta, Georgia 30067  
**Telephone:** (404) 641-9632 **Email:** [balbonag@mac.com](mailto:balbonag@mac.com)

June 26, 2017

**PETITION FOR RECANVASS BY ELECTORS IN THE 6<sup>th</sup> DISTRICT OF GEORGIA**

We, citizens of the 6<sup>th</sup> District of DeKalb County, Georgia, hereby petition a recanvass of all the memory cards (PCMCIA cards) for the following precincts in DeKalb County:

Briarwood  
Ashford Park Elem  
Kittredge Elem  
Cross Keys High  
Mt Vernon West

Recounts and Recanvasses are governed by the Rules of the State Election Board of Georgia, Ga Comp. R. & Regs. 183-1-12-01:

- (7) Recounts and Recanvass.
  - (a) The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made. Such recanvass may be held at any time prior to the certification of the consolidated returns by the election superintendent and shall be conducted under the direction of the election superintendent. Before making such recanvass, the election superintendent shall give notice in writing to each

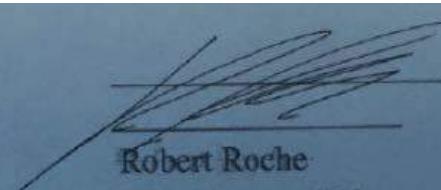
candidate and to the county chairperson of each party or body affected by the recanvass. Each such candidate may be present in person or by representative and each such political party or body may send two representatives to be present at such recanvass. If upon such recanvass, it shall appear that the original vote count was incorrect, such returns and all papers being prepared by the election superintendent shall be corrected accordingly.

- (b) The election superintendent shall conduct the recanvass by breaking the seal, if the ballots cards have been sealed, on the container containing the memory cards (PCMCIA cards) and removing those memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted. The election superintendent shall then cause the vote totals on each of the memory cards (PCMCIA cards) to be transferred to either an accumulator DRE unit or to the election management system computer. After all of the vote totals from the memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted have been entered, the election superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If an error is found, the election superintendent shall correct the error in the returns accordingly.

We, three electors of the 6<sup>th</sup> District in DeKalb County, Georgia, hereby petition for a recanvass of all of the memory cards for the aforementioned precincts because they may contain errors and discrepancies, which must be examined and corrected.

Respectfully submitted,

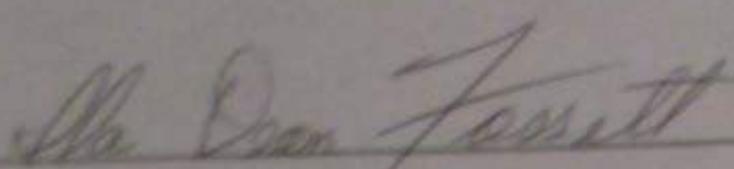
George Balbona

  
July 25, 2017

Robert Roche  
3633 Chestnut Drive  
Doraville, Ga 30340  
DeKalb County

I agree with this petition and am happy to contractually and legally bindingly add my signature via this email.

John R. Pastor  
3563 Sexton Woods Dr.  
Chamblee, Ga.  
30341

  
Ila DEAN FOSSETT  
1791 HICKORY ROAD  
CHAMBLEE, GA 30341

**George Balbona**  
180 Mathews Circle, Marietta, Georgia 30067  
**Telephone:** (404) 641-9632 **Email:** [balbonag@mac.com](mailto:balbonag@mac.com)

June 26, 2017

**PETITION FOR RECANVASS BY ELECTORS IN THE 6<sup>th</sup> DISTRICT OF GEORGIA**

We, citizens of the 6<sup>th</sup> District of Cobb County, Georgia, hereby petition a recanvass of all the memory cards (PCMCIA cards) for the following precincts in Cobb County:

|                  |                 |                 |
|------------------|-----------------|-----------------|
| Chattahoochee 01 | Bells Ferry 03  | Eastside 01     |
| Marietta 5A      | Roswell 01      | Fullers Park 01 |
| Marietta 6A      | Mount Bethel 01 |                 |
| Marietta 6B      | Hightower 01    |                 |
| Marietta 7A      | Eastside 02     |                 |
| Powers Ferry 01  | Murdock 01      |                 |

Recounts and Recanvasses are governed by the Rules of the State Election Board of Georgia, Ga Comp. R. & Regs. 183-1-12-.01:

**(7) Recounts and Recanvass.**

- (a)** The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made. Such recanvass may be held at any time prior to the certification of the consolidated returns by the election superintendent and shall be conducted under the direction of the election superintendent. Before making such recanvass, the

election superintendent shall give notice in writing to each candidate and to the county chairperson of each party or body affected by the recanvass. Each such candidate may be present in person or by representative and each such political party or body may send two representatives to be present at such recanvass. If upon such recanvass, it shall appear that the original vote count was incorrect, such returns and all papers being prepared by the election superintendent shall be corrected accordingly.

- (b) The election superintendent shall conduct the recanvass by breaking the seal, if the ballots cards have been sealed, on the container containing the memory cards (PCMCIA cards) and removing those memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted. The election superintendent shall then cause the vote totals on each of the memory cards (PCMCIA cards) to be transferred to either an accumulator DRE unit or to the election management system computer. After all of the vote totals from the memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted have been entered, the election superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If an error is found, the election superintendent shall correct the error in the returns accordingly.

We, three electors of the 6<sup>th</sup> District in Cobb County, Georgia, hereby petition for a recanvass of all of the memory cards for the aforementioned precincts because they may contain errors and discrepancies, which must be examined and corrected.

Respectfully submitted,



George Balbona

George Balbona

George Balbona



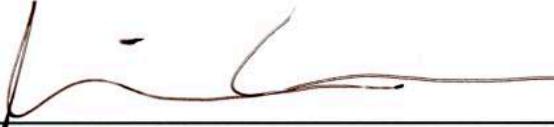
ALLISON KNOCH  
NOTARY PUBLIC  
GWINNETT COUNTY, GEORGIA  
MY COMMISSION EXPIRES  
DECEMBER 21, 2017

---

Sworn to and submitted before me this 25<sup>th</sup> day of June, 2017.

Cathy Balbona

Cathy Balbona



ALLISON KNOCH  
NOTARY PUBLIC  
GWINNETT COUNTY, GEORGIA  
MY COMMISSION EXPIRES  
DECEMBER 21, 2017

---

Sworn to and submitted before me this 25<sup>th</sup> day of June, 2017.



---

Brian Peters



ALLISON KNOCH  
NOTARY PUBLIC  
GWINNETT COUNTY, GEORGIA  
MY COMMISSION EXPIRES  
DECEMBER 21, 2017

---

Sworn to and submitted before me this 25<sup>th</sup> day of June, 2017.

## EXHIBIT K

**Rocky Mountain Foundation**

7035 Marching Duck Drive E504  
Charlotte, NC 28210  
704 552 1518

Marilyn@RockyMountainFoundation.org

June 24, 2017

Fulton County Board of Elections  
Hand delivered  
(Also via email felisa.cordy@fultoncountyga.gov  
richard.barron@fultoncountyga.gov  
Dwight.Brower@fultoncountyga.gov )

Dear Fulton County Board of Elections:

As you consider the certification of the 6<sup>th</sup> Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. Fulton County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct of the Superintendent and staff by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, Fulton County officials have been aware of gravely concerning security failures and intrusions, and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in

the June 7 Curling v. Kemp et al. hearing that the security lapses render the system insecure and unfit for the conduct of the election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server.

(<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) Fulton officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. On April 18, Fulton County officials exposed the GEMS server and all memory cards to cyber security attack from the Internet by using a common, shared flash drive to upload from the GEMS server to the on-line Clarity ENR system, and then reusing that flash drive in the GEMS server. Such serious lapses in security hygiene must be presumed to have compromised the system, and constitute misconduct on the part of the officials. It cannot be reasonably assumed that the system was safe for vote recording and tabulation, even if this practice had been discontinued on June 20. Exposure to the Internet via shared flash drives undermined the security of the entire election.

Although regulations require direct upload of memory cards to the GEMS server for official results with the stated intent of avoiding cyber-attacks in election night electronic transmission, the poor security hygiene practices in Fulton County only escalate the risk of cyber-attack. The memory cards and the GEMS server were exposed and made vulnerable during the election night electronic transmission and during the physical upload to the GEMS server after the GEMS server was exposed to the Internet through the irresponsible use of shared flash-drives. Such misconduct cannot be ignored by this board.

3. The Fulton County collection centers' use of TSx machines to transmit votes from TS machines over modem is not a federally approved standard use of the TSx machine, and not certified to be configured, connected and used in this manner, which exposes the memory cards and GEMS server to cyber-attacks during electronic transmission.
4. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as required by statute, nor have such certifications covered the current system configuration. Fulton County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.

5. Physical security of the machines was inadequate prior to the election and during early voting. Given the known exposure of Georgia's system to cyber-attacks and the risk of undetected hacking, it was irresponsible of Fulton County Board and Superintendent to leave machines exposed to easy access by malicious intruders cutting cables and using and replacing tamper-evident seals with identical seals. Although current regulations may permit such risky machine storage in unsecured areas, the board must not irresponsibly rely on permissive and outdated regulations when grave security risks are known to exist. Responsible decisions must be made in light of existing circumstances. If a hallway were flooded with water, machines would not be placed in the water just because the regulations don't prohibit putting machines in flooded areas. Officials have a duty to protect the voting system, and have failed in that duty, in a negligent abuse of discretion.
6. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."
7. On April 18, Fulton County experienced memory card uploading problems to the GEMS server. Officials stated that the GEMS server displayed a message that the upload was successful, with no error messages received until the export of the data from GEMS to the Clarity system. The Superintendent and Board are aware that a functioning, certified GEMS server produces error messages. and does not permit the upload of improper memory cards. This serious problem of no error message signals that the GEMS server is not in safe and proper operational condition, and cannot be relied on to generate accurate election results.
8. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Superintendent must fulfil their legal duty to conduct a secure election free from the threats of a compromised system.
9. Despite the Superintendent's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Superintendent abused his discretion by ignoring multiple expert warnings and conducting the election on a system he knew to be insecure and in violation of laws and regulations. Mr. Barron was present for testimony in the June 7 Curling v. Kemp hearing, and received the pleading including experts' affidavits in that case, and therefore had more than adequate knowledge of the dangers of the uncertified system to require that he employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified. It supplements the petition for paper ballots delivered to this board on May 11. (attached.)

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,



Marilyn Marks  
Executive Director  
Rocky Mountain Foundation

**Rocky Mountain Foundation**

7035 Marching Duck Drive E504  
Charlotte, NC 28210  
704 552 1518

Marilyn@RockyMountainFoundation.org

June 26, 2017

Director Daniels and DeKalb County Board of Elections  
Hand delivered  
(Also via email [voterreg@dekalbcountyga.gov](mailto:voterreg@dekalbcountyga.gov) )

Dear Director Daniels and DeKalb County Board of Elections:

As you consider the certification of the 6<sup>th</sup> Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were eligible voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up to the election. DeKalb County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election, or the results you plan to certify today.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, DeKalb County officials have been aware of gravely concerning security failures and intrusions, (particularly those at KSU), and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in the June 7 Curling v. Kemp et al. hearing that the security lapses render the system insecure and unfit for the conduct of the

election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server.

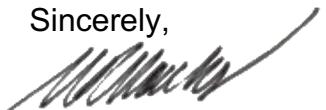
(<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) DeKalb officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. DeKalb County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.
3. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."
4. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Elections Director must fulfil their duty to conduct a secure election free from the threats of a compromised system.
5. Despite the Board's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Director and Board abused their discretion by ignoring multiple expert warnings and conducting the election on a system she knew to be insecure and in violation of laws and regulations. The board was represented by attorneys for testimony in the June 7 Curling v. Kemp hearing, and received the pleadings in that case, and therefore had more than adequate knowledge of the dangers of the uncertified and compromised system to require that Ms. Daniels and the board employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified.

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,



Marilyn Marks  
Executive Director  
Rocky Mountain Foundation

cc: Bennett Bryan (bdbryan@dekalbcountyga.gov )

**Rocky Mountain Foundation**

7035 Marching Duck Drive E504  
Charlotte, NC 28210  
704 552 1518

Marilyn@RockyMountainFoundation.org

June 26, 2017

Director Eveler and Cobb County Board of Elections  
Hand delivered  
(Also via email dwhite@hlclaw.com)

Dear Director Eveler and Cobb County Board of Elections:

As you consider the certification of the 6<sup>th</sup> Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were eligible voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. Cobb County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election, or the results you plan to certify today.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct of the Superintendent and staff by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, Cobb County officials have been aware of gravely concerning security failures and intrusions, and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in the June 7 Curling v. Kemp et al. hearing that the security lapses render the

system insecure and unfit for the conduct of the election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server.

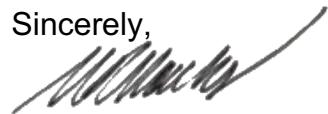
(<http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255>) Cobb officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. Cobb County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.
3. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."
4. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Elections Director must fulfil their duty to conduct a secure election free from the threats of a compromised system.
5. Despite the Director's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Director abused her discretion by ignoring multiple expert warnings and conducting the election on a system she knew to be insecure and in violation of laws and regulations. Ms. Eveler was present for testimony in the June 7 Curling v. Kemp hearing, and received the pleadings in that case, and therefore had more than adequate knowledge of the dangers of the uncertified and compromised system to require that she employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified.

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,



Marilyn Marks  
Executive Director  
Rocky Mountain Foundation

cc: Daniel W. White ([dwhite@hlclaw.com](mailto:dwhite@hlclaw.com) )